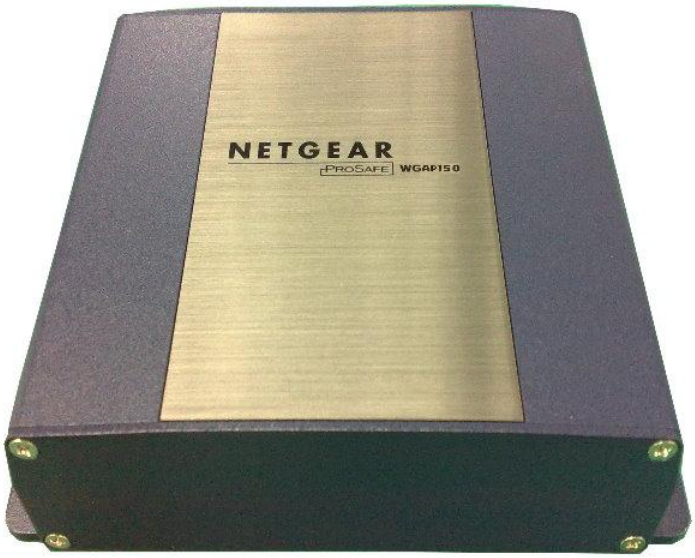
NETGEAR

WG102-500, WGAP150 ProSafe™ 802.11g Wireless Access Point

Reference Manual



350 East Plumeria Drive
San Jose, CA 95134
USA

December 2010
202-10755-01
1.1

©2010 NETGEAR, Inc. All rights reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, or get support online, visit us at http://support.netgear.com.

Phone (US & Canada only): 1-888-NETGEAR

Phone (Other Countries): See Support information card.

Trademarks

NETGEAR, the NETGEAR logo, ReadyNAS, ProSafe, Smart Wizard, Auto Uplink, X-RAID2, and NeoTV are trademarks or registered trademarks of NETGEAR, Inc. Microsoft, Windows, Windows NT, and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10755-01	1.1	December 2010	Removed Resource CD

Table of Contents

Chapter 1 Introduction

About the Wireless Access Point 7
Supported Features, Standards, and Conventions 8
Supported Standards and Conventions 8
Key Features 8
802.11g Standards-based Wireless Networking 9
Wi-Fi Multimedia (WMM) Support 9
System Requirements 10
What's In the Box? 10
Hardware Description 11
Rear Panel 11
Recommendations for Placement of the Wireless Access Point 12

Chapter 2 Installation and Basic Configuration

What You Need before You Begin 13
Wireless Equipment Placement and Range Guidelines 13
Ethernet Cabling Requirements 14
LAN Configuration Requirements 14
Computer Hardware Requirements 15
Installing and Configuring the Wireless Access Point 15
Connecting the Wireless Access Point to Computer 15
Logging in to the Wireless Access Point 17
Web Interface Menu 18
Configuring Basic System Settings, IP Settings, and LAN Settings 18
Configuring Basic System Settings 19
Configuring IP Settings 20
Configuring LAN Settings 23
Configuring Basic Wireless Settings 24
Configuring 802.11b/g Wireless Settings 25
Configuring Basic Wireless Network Settings 27
Testing Basic Wireless Connectivity 31

Chapter 3 Wireless Configuration and Security

Wireless Data Security Options 33
Security Profiles 35
Before You Change the SSID, WEP, and WPA Settings 36
Creating and Editing Security Profiles 37
Configuring Static WEP 40
Configuring Legacy 802.1X (or Dynamic WEP) 41
Configuring WPA and WPA-PSK (TKIP) 41
Configuring WPA2 and WPA2-PSK (AES) 43
Configuring WPA+WPA2 / WPA-PSK+WPA2-PSK Mixed Modes . . 44
Configuring RADIUS Server Settings 45
Configuring General RADIUS Server Settings 45
Configuring Alternate RADIUS Server Settings 48
Selecting the 802.1x EAPOL Version 48
WAPI Certificates 49
Restricting Wireless Access by MAC Address 50
Configuring Alternate DHCP Server Settings 52
Configuring Wireless Quality of Service 54
Configuring Wireless Traffic Shaping 54
Configuring Wireless Traffic Filtering 55
Configuring Advanced QoS Settings 57
Configuring Wireless Client Separation 58
Globally Enabling Wireless Client Configuration 58
Refining Wireless Client Separation 58

Chapter 4 Managing Your Network

Backing Up, Restoring, and Erasing Your Settings 61
Backing up the Configuration 62
Restoring the Configuration 62
Rebooting and Restoring the Default Configuration 63
Using the Software to Reboot and Restore Factory Defaults 63
Using the Reset Button to Reboot and Restore Factory Default . . . 63
Saving the Configuration to Flash Memory 63
Scheduling to Activate the Changes 64
Rebooting without Restoring the Default Configuration 64
Upgrading the Wireless Access Point Firmware 65
Changing the Administrator Password and User Name 66
Changing the Administrator Password 66
Changing the Administrator User Name 67
Viewing Network Management Information 68
Viewing the Activity Log 68
Viewing the Activity Log on Screen 68
Sending the Activity Log to a Syslog Server 69
Viewing System Information 70
Viewing the Basic System Information Screen 71
Viewing the L2TP Tunnel Information Screen 73

Viewing the Flash Management Information Screen 74
Viewing Wireless Information 74
Viewing the Basic Wireless Information Screen. 75
Viewing the Wireless Clients Information Screen 75
Viewing Neighbor APs Information 76
Configuring Remote Management 78
Web Management Access 78
Configuring Web Management Access 78
Disabling Web Management Access from Wireless Clients 80
Disabling Web Management Access Entirely 81
Configuring L2TP Tunnel Management 82
Configuring Telnet Server Access 84
SNMP Remote Management 85
Configuring SNMP Settings 85
Configuring SNMP Communities 86
Configuring SNMP Users 88
Configuring TR069 Operation. 90
Scheduling Management Tasks 91
Accessing Online Documentation. 93

Chapter 5 Advanced Configuration

Accessing Online Documentation. 93
Configuring Ethernet Links 95
Configuring Hotspots (Captive Portals) 96
Configuring Advanced Wireless Settings 98
Configuring Neighbor AP Discovery 101
Configuring Wireless Bridging and Repeating 102
Configuring Point-to-Point Bridge Mode 104
Configuring Point to Multi-Point Bridge Mode. 106
Configuring Repeater Mode 108

Chapter 6 Troubleshooting

Basic Functioning 112
No LEDs are Lit on the Wireless Access Point 112
The LAN LED is Not Lit 112
The Wi-Fi LED Does Not Light Up During Wireless Activity 112
You Cannot Access the Internet or the LAN from a Wireless-Capable Computer 113
You Cannot Configure the Wireless Access Point from a Browser 113
When You Enter a URL or IP Address a Time-out Error Occurs 114
Troubleshooting a TCP/IP Network Using the Ping Utility 114
Testing the LAN Path to Your Wireless Access Point 115
Testing the Path from Your Computer to a Remote Device 115
Using the Reset Button to Restore Factory Default Settings 116
Problems with Date and Time 116
Using the Diagnostic Tools 117
Health Check 117
Using the Ping, Traceroute, and NsLookup Utility 118
Downloading Debug Information 119

Appendix A Technical Specifications

General Specifications 121
Default Factory Settings 122

Appendix B Related Documents

Index

1 Introduction

The *NETGEAR® WG102-500, WGAP150 ProSafe™ 802.11g Wireless Access Point Reference manual* describes how to install, configure and troubleshoot the wireless access point. The information in this manual is intended for readers with intermediate computer and Internet skills

The remainder of this chapter introduces the wireless access point. Minimal requirements for installation are on page 10.

About the Wireless Access Point

The wireless access point is the basic building block of a wireless LAN infrastructure. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices.

The wireless access point interacts with wireless network interface cards (NIC) in wireless devices within a fixed range or area of coverage. Typically, a wireless access point inside a building works best with devices within a 100 foot radius. The WGAP150 can support a small group of users in a range of several hundred feet. Most wireless access points are rated between 30 users simultaneously.

Note: The WGAP150 requires an external antenna to be connected to the WGAP150 before powering on the access point. An external antenna is not included in the product package and must be purchased separately. The environment in which you deploy the WGAP150 determines the type of antenna that functions best with the WGAP150.

The WGAP150 acts as a bridge between the wired LAN and wireless clients. Connecting multiple WGAP150 access points via a wired Ethernet backbone can further lengthen the wireless network coverage. As a mobile computing device moves out of the range of one wireless access point, it moves into the range of another. As a result, wireless clients can freely roam from one wireless access point to another and still maintain seamless connection to the network.

Supported Features, Standards, and Conventions

The WGAP150 is easy to use and provides complete wireless and networking support.

Supported Standards and Conventions

The following standards and conventions are supported:

- **Standards Compliant**. The wireless access point complies with the IEEE 802.11n for Wireless LANs.
- **WEP support**. Support for WEP is included. 64-bit, 128-bit, and 152-bit keys are supported.
- **Full WPA and WPA2 support**. WPA and WPA2 enterprise class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation. WPA-PSK and WPA2-PSK pre-shared key authentication without the overhead of RADIUS servers but with all of the strong security of WPA.
- **DHCP Client Support**. DHCP provides a dynamic IP address to PCs and other devices upon request. The WGAP150 can act as a client and obtain information from your DHPC server.
- **Multiple BSSIDs**. Support for multiple BSSIDs. When one AP is connected to a wired network and a set of wireless stations it is referred to as a Basic Service Set (BSS). The wireless access point supports multiple wireless security profiles, each with their own Service Set Identifier (SSID) and Basic SSID (BSSID). The SSID and BSSID are attached to the header of packets sent over a WLAN to differentiate one WLAN from another when a mobile device tries to connect to the network. The BSSID for a wireless security profile consist of the MAC address of the wireless access point with the last digit altered.
- **SNMP Support**. Support for Simple Network Management Protocol (SNMP) Management Information Base (MIB) management.

Key Features

The WGAP150 provides solid functionality, including these features:

- **Choice of Operating Modes**
  - **Wireless Access Point**. Operates as a standard 802.11n wireless access point.
  - **Wireless Distribution System**. You can build large bridged wireless networks by using the wireless access point to configure a wireless distribution system (WDS). The wireless access point can be configured to function as a point-to-point bridge, point-to-multi-point bridge, or wireless repeater.
- **Hotspot Capability**. HTTP requests can be captured and redirected.
- **Upgradeable Firmware**. Firmware is stored in a flash memory and can be upgraded easily using only your Web browser, or remotely with a CLI or through SNMP.

- **Access Control**. The Access Control MAC address filtering feature can ensure that only trusted wireless stations can use the WGAP150 to gain access to your LAN.
- **Security Profiles**. When using multiple BSSIDs, you can configure unique security settings (encryption, MAC filtering, etc.) for each BSSID.
- **Wireless Quality of Service**. When using multiple BSSIDs, you can allocate quality of service (QoS) levels, set traffic bandwidth limits, and configure advanced QoS settings for each BSSID.
- **Simple Configuration**. If the default settings are unsuitable, they are easy to change.
- **Hidden Mode**. In this mode, the SSID is not broadcast, assuring only clients configured with the correct SSID can connect.
- **Configuration Backup**. Configuration settings can be backed up to a file and restored.
- **Ethernet Interface**. Connects to 10/100 Mbps IEEE 802.3 Ethernet networks.
- **Power over Ethernet**. Power must be supplied to the access point over the Ethernet port from any 802.3af compliant mid-span or end-span source such as the NETGEAR FSM7326P Managed Power over Ethernet Layer 3 managed switch.
- **LED Indicators**. Power, LAN activity, and wireless activity are easily identified.
- **VLAN Support**. Short for a virtual LAN, a network of computers that behave as if they are connected to the same network even though they may actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. VLANs are very useful for user/host management, bandwidth allocation and resource optimization.

802.11g Standards-based Wireless Networking

The WGAP150 provides a bridge between Ethernet wired LANs and 802.11g compatible wireless LAN networks. The WGAP150 also supports the following wireless features:

- Distributed coordinated function (CSMA/CA, Back off procedure, ACK procedure, retransmission of unacknowledged frames)
- RTS/CTS handshake
- Beacon generation
- Packet fragmentation and reassembly
- Short or long preamble
- Roaming among wireless access points on the same subnet

Wi-Fi Multimedia (WMM) Support

WMM is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video or audio, has a higher priority than normal traffic. For WMM to function correctly, wireless clients must also support WMM.

System Requirements

Before installing the WGAP150, make sure your system meets these requirements:

- A category 5 UTP straight-through Ethernet cable with RJ-45 connector.
- An external antenna.
- A Web browser for configuration such as Microsoft Internet Explorer 6.0 or above, or Mozilla Firefox 1.5 or above.
- At least one computer with the TCP/IP protocol installed.
- 802.11b/g compliant devices, such as the NETGEAR WG511, WG111, or WN111 Wireless Adapters.

What's In the Box?

The product package should contain the following items:

- NETGEAR WG102-500, WGAP150 ProSafe™ 802.11g Wireless Access Point
- Power adapter and cord
- Straight-through category 5 Ethernet cable
- Installation Guide
- Support registration card

Contact your reseller or customer support in your area if there are any missing or damaged parts. See the Support Information Card for the telephone number of customer support in your area. You should keep the Support Information card, along with the original packing materials, and use the packing materials to repack the WGAP150 if you need to return it for repair. To qualify for product updates and product warranty registrations, we encourage you to register on the NETGEAR Web site at: *http://www.netgear.com*.

Hardware Description

The following figure shows a top view of the WGAP150

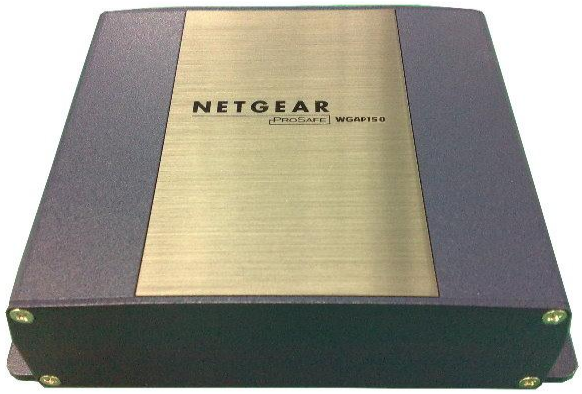


Figure 1-1

Rear Panel

The following figure shows a rear panel view of the WGAP150:

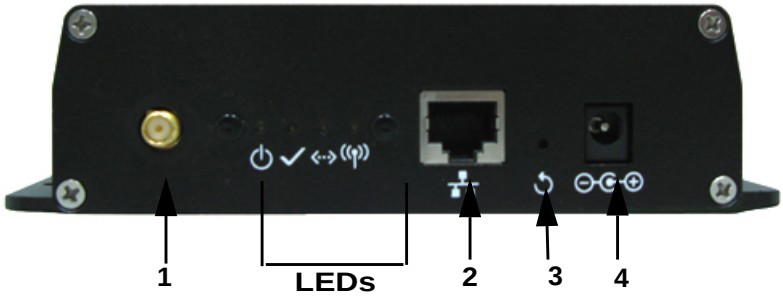


Figure 1-2

Viewed from left to right, the rear panel of the WGAP150 provides the following connectors and buttons:

1. **Antenna**. An RP-SMA connector for connecting an external antenna, which does not come standard with the WGAP150.
2. **LAN Connector**. A 10/100BaseT Ethernet connector, normally to be connected to a back haul network.
3. **Reset Button**. A reset button to be depressed with a pin. Depress and hold for at least 5 seconds to restore factory defaults. (For more information, see “Rebooting and Restoring the Default Configuration” on page 63.)
4. **Power Connector**. A connector for 12 VDC power input, to be connected with the supplied power adaptor.

Viewed from left to right, the WGAP150 has these four status LEDs: Power, Status, Ethernet, and Wi-Fi (also referred to as WLAN light or Wireless activity light):

Table 1-1.

LED	Activity	Description
Power	Off	Power off
	On (Green)	Power on
Status	Off	The unit is initializing.
	On (Green)	The unit is ready.
LAN	Off	The Ethernet port is not connected.
	On	The Ethernet port is connected.
Wi-Fi	Off	Wireless is not ready.
	On	Wireless is ready.

Recommendations for Placement of the Wireless Access Point

The following are recommendations for the placement of the wireless access point and the positioning of its antenna:

- The best location for the wireless access point is elevated, such as wall mounted or on the top of a cubicle, at the center of your wireless coverage area, and within line of sight of all the mobile devices.
- Vertical positioning of the antenna provides best side-to-side coverage. Horizontal positioning provides best top-to-bottom coverage.

Installation and Basic Configuration

2

This chapter describes how to install and configure your access point for wireless connectivity to your LAN. This basic configuration will enable computers with 802.11b/g or 802.11n wireless adapters to connect to the Internet, or access printers and files on your LAN. In planning your wireless network, consider the level of security required. *Chapter 3* describes how to set up wireless security for your network.

> **Note:** In this chapter and in all further chapters, the WGAP150 is referred to as the wireless access point.

This chapter includes:

- *What You Need before You Begin* ” on this page
- *“Installing and Configuring the Wireless Access Point” on page 15*
- *“Testing Basic Wireless Connectivity” on page 31*

What You Need before You Begin

You need to consider the following guidelines and requirements before you can set up your wireless access point. See also *“System Requirements” on page 15*.

Wireless Equipment Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the location of the wireless access point. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the wireless access point. For complete performance specifications, see *Appendix A*.

For best results, place your wireless access point according to the following general guidelines:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwaves ovens, and 2.4 GHz cordless phones.
- Away from large metal surfaces or water.
- Placing an external antenna in a vertical position provides best side-to-side coverage. Placing an external antenna in a horizontal position provides best up-and-down coverage. (An external antenna does not come standard with the WGAP150.)
- If using multiple wireless access points, it is better if adjacent wireless access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent wireless access points is five channels (for example, use channels 1 and 6, or 6 and 11, or 1 and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings, and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Ethernet Cabling Requirements

The wireless access point connects to your LAN via twisted-pair category 5 Ethernet cable with RJ-45 connectors.

LAN Configuration Requirements

For the initial configuration of your wireless access point, you need to connect a computer to the wireless access point.

Note: For assistance with DHCP configuration, see the online document that you can access from "Preparing Your Network" in Appendix B.

Computer Hardware Requirements

To connect to the wireless access point on your network, each computer must have a 802.11b/g or 802.11n wireless adapter installed.

Installing and Configuring the Wireless Access Point

Before installing the wireless access point, make sure that your Ethernet network is up and working. You will be connecting the wireless access point to the Ethernet network. Then computers with 802.11b/g or 802.11n wireless adapters will be able to communicate with the Ethernet network.

In order for this to work correctly, verify that you have met all of the system requirements, shown in *"System Requirements" on page 10*.

Install and configure your wireless access point in the order of the following sections:

1. *Connecting the Wireless Access Point to Computer* " on this page.
2. *"Logging in to the Wireless Access Point" on page 17*.
3. *"Configuring Basic System Settings, IP Settings, and LAN Settings" on page 18*.
4. *"Configuring Basic Wireless Network Settings" on page 27*.

Connecting the Wireless Access Point to Computer

To set up the wireless access point:

> **Tip:** Before you place the wireless access point in an elevated position that is difficult to reach, first set up and test the wireless access point to verify wireless network connectivity.

1. Unpack the box and verify the contents.
2. Prepare a computer with an Ethernet adapter. If this computer is already part of your network, record its TCP/IP configuration settings. Configure the computer with a static IP address of 192.168.0.210 and 255.255.255.0 as the subnet mask.
3. Connect an Ethernet cable from the wireless access point to the computer (point A in Figure 2-1 on page 16).
4. Securely insert the other end of the cable into the wireless access point's Ethernet port (point B in Figure 2-1 on page 16).

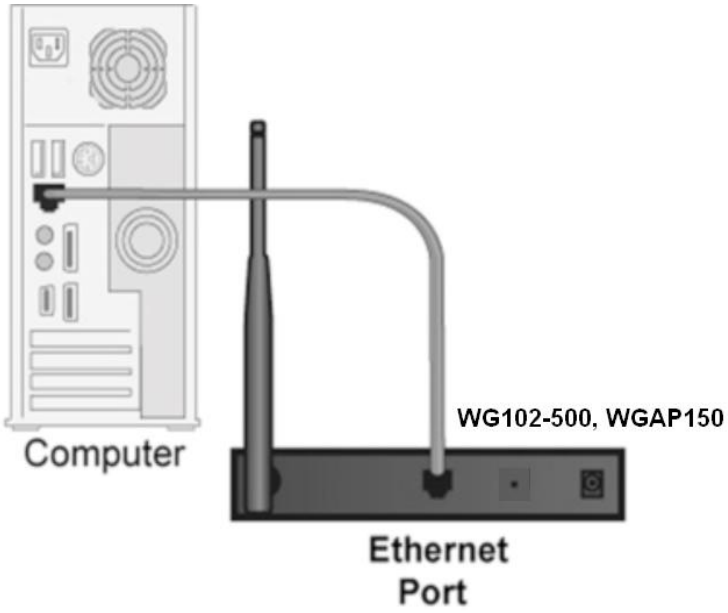


Figure 2-1

Note: *Figure 2-1* shows the WGAP150 with an external antenna, which does not come standard with the product.

5. Turn on your computer, connect the power adapter to the wireless access point and verify the following:

   Power LED. The powerLEDt on the wireless access point should be steady green. If the power light is not lit, check the connections, and check if the power outlet is controlled by a wall switch that is turned off.

   Status LED. The status LED on the wireless access point should be blinking red while the wireless access point starts up. When the startup process is complete, the status LED should be steady green to indicate the access point is ready.

   LAN LED. The LAN LED on the wireless access point should be blinking green. If it is not, make sure that the Ethernet cable is securely attached at both ends.

   Wi-Fi LED. The Wi-Fi LED on the wireless access point should be blinking green when the wireless LAN (WLAN) is ready.

Tip: The wireless access point supports Power Over Ethernet (PoE). If you have a switch that provides PoE, you will not need to use the power adapter to power the wireless access point. This can be especially convenient when the wireless access point is installed in a high location far away from a power outlet.

Logging in to the Wireless Access Point

The default IP address of your wireless access point is 192.168.0.229. The wireless access point is set, by default, for the DHCP client to be disabled.

To log in to the wireless access point:

1. Open a Web browser such as Microsoft Internet Explorer 6.0 or above, or Mozilla Firefox 1.5 or above.
2. Connect to the wireless access point by entering its default address of **http://192.168.0.229** into your browser:

Figure 2-2

The Login screen opens.

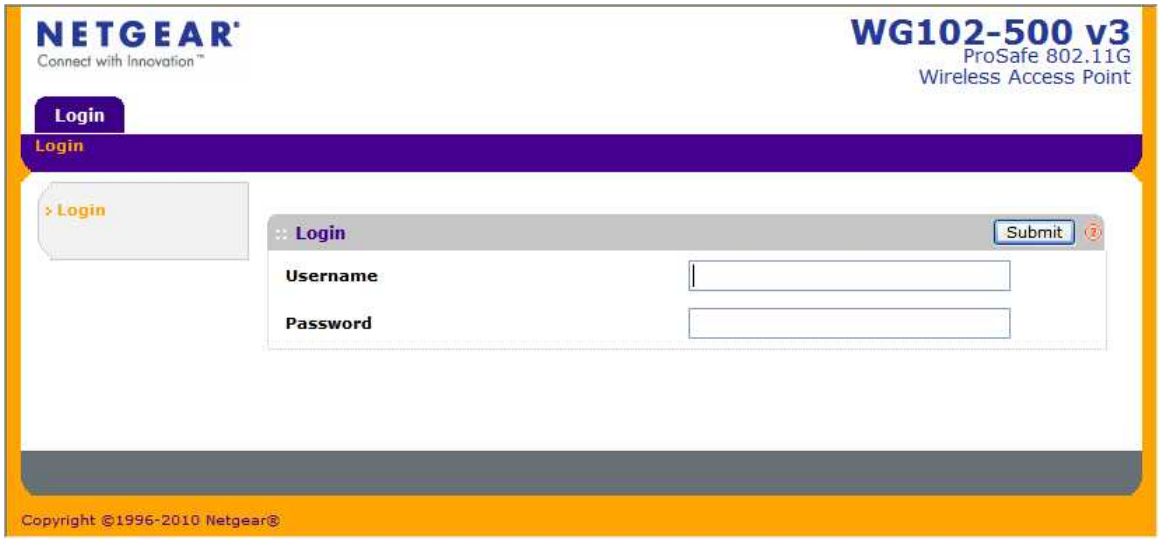


Figure 2-3

3. Enter the default user name of **admin** and the default password of **password**.
4. Click **OK**. The Web browser displays the Basic General Settings screen under the Configuration tab of the main menu as shown in Figure 2-6 on page 19.

Web Interface Menu

The navigation tabs across the top of the Web interface menu provide access to all the configuration functions of the wireless access point, and remain constant. The menu items in the blue bar change according to the navigation tab that is selected.

Figure 2-4

The bottom right corner of the Basic Settings screen and any other screen that allows you to make configuration changes shows the Save and Save to Flash & Activate buttons.

Figure 2-5

These buttons have the following functions:

- **Save**. Saves any configuration changes but does not activate the new configuration, and the changes are lost when you reload the wireless access point.
- **Save to Flash & Activate**. Activates any configuration changes and saves them to the flash memory, allowing the changes to remain active after the wireless access point has been reloaded.

Configuring Basic System Settings, IP Settings, and LAN Settings

The Basic Settings screen consists of three sections: Basic System Settings, IP Settings, and LAN Settings. Depending on the selections that you make, the IP Settings section and the LAN Settings section shows different fields for you to configure.

To open the Basic Settings screen, log in to the wireless access point as described in “Logging in to the Wireless Access Point” on page 17. The Web browser displays the Basic

Settings screen (see Figure 2-6 on page 19). The full path to this screen is **Configuration** > **System** > **Basic**.

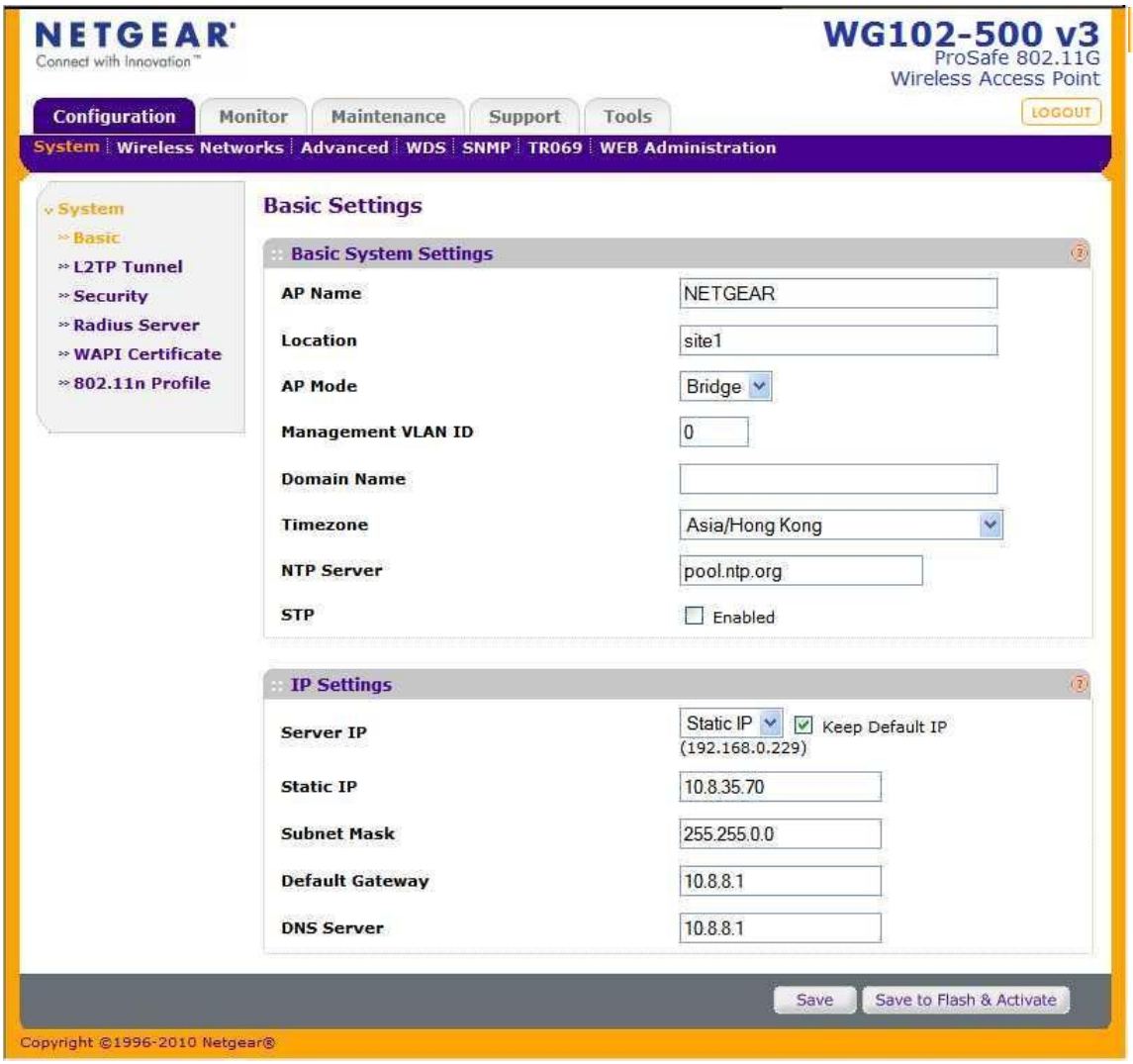


Figure 2-6

Configuring Basic System Settings

To configure the basic system settings:

1. Specify the fields in the Basic System Settings section of the Basic Settings screen (see *Figure 2-6*) as explained in *Table 2-1*.

Table 2-1. Basic System Settings

Field	Description	
AP Name	Assign a unique name to the wireless access point.The default name is NETGEAR. The AP name can be retrieved through SNMP.	
Location	Assign a unique name to the location of the wireless access point.The default name is site1. The site name can be retrieved through SNMP.	
AP Mode	Select one mode from the pull-down menu: • **Bridge**. The wireless access point functions as a bridge, for example, between a wired and a wireless network. This is the default setting. • **Router**. The wireless access point functions as a router. When you select this mode, the Management VLAN ID becomes inactive and the LAN settings appear at the bottom of the Basic Settings screen (see "Configuring LAN Settings" on page 23).	
Management VLAN ID	The management VLAN can be active only when the wireless access point functions as a bridge. Specify a VLAN ID from which the wireless access point can be managed. The default setting is zero, which allows for management of the wireless access point from any VLAN, and which prevents frames belonging to the Management VLAN from being tagged with an 802.1Q header when sent over the trunk.	
Domain Name	Select an easily recognizable domain name to facilitate web management and the redirection of HTTP requests.	
Time Zone	Select the time zone to match your location.	
NTP Server	If you want to use a Network Time Protocol (NTP) server, enter its host name. **Note**: You must have an Internet connection to use an NTP server that is not on your local network.L	
STP	Select the **STP** checkbox to enable the Spanning Tree Protocol (STP) to prevent path redundancy. When the STP checkbox is selected, two more options appear on the Basic Settings screen.	
	Bridge Priority	Enter the priority for root switch election. The default is 32768.
	Ethernet Path Cost	Enter the best path cost from the switch to the root switch. The default is 100.

2. Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring IP Settings

To configure the IP settings:

1. Specify how the wireless access point acquires its IP address by making a selection from the **Server IP** pull-down menu in the IP Settings section of the Basic Settings screen (see Figure 2-7 on page 21):
   - **DHCP**. The IP address, subnet mask, and the default gateway settings for the wireless access point are acquired automatically from a Dynamic Host Configuration

Protocol (DHCP) server on the Ethernet segment (see “Configuring LAN Settings” on page 23). This is the default settings; no further configuration is required.

- **Static IP**. Your Internet Service Provider (ISP) has assigned you a permanent, fixed (static) IP address. When you select Static IP, the IP Settings section of the Basic Settings screen expands:

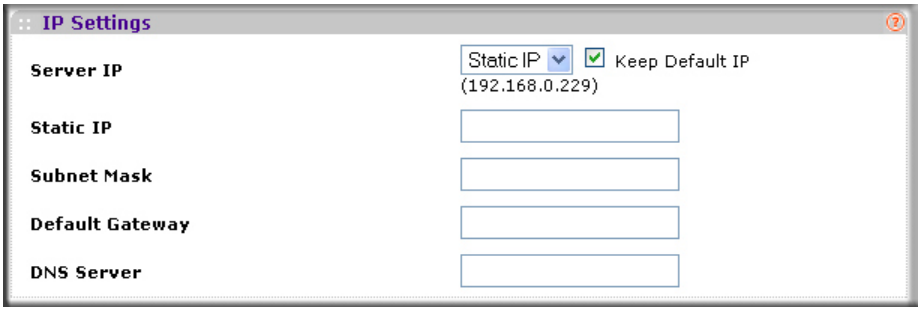


Figure 2-7

Specify the static IP fields as explained in *Table 2-2*.

Table 2-2. Static IP Settings

Field	Description
Static IP	The fixed IP address that your ISP has assigned to you.
Subnet Mask	The network number portion of an IP address. Unless you are implementing subnetting, use 255.255.0.0 as the subnet mask.
Default Gateway	The ISP’s router to which the wireless access point will connect.
DNS Server	A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your wireless access point during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually in this field.

- **PPPoE**. You connect to your ISP over a PPP over Ethernet (PPPoE) line, and your ISP has assigned you a user name, password, and, possibly, a service name. The PPPoE mode is available only if you selected “Router” as the AP mode (see “Configuring Basic System Settings” on page 19). When you select PPPoE, the IP Settings section of the Basic Settings screen expands (see Figure 2-8 on page 22).

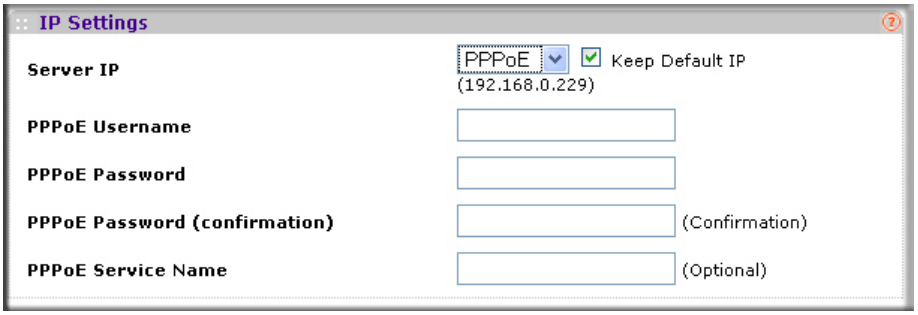


Figure 2-8

Specify the PPPoE fields as explained in *Table 2-3*.

Table 2-3. PPPoE Settings

Field	Description
PPPoE Username	The PPPoE user name that your ISP has assigned to you.
PPPoE Password	The PPPoE password that your ISP has assigned to you.
PPPoE Password (confirmation)	Repeat the PPPoE password that your ISP has assigned to you.
PPPoE Service Name	The PPPoE service name that your ISP has assigned to you. If your ISP did not assign you a service name, leave this field blank.

2. If you want to use the default IP address of the wireless access point (192.168.0.229) and the default server IP settings that are defined in “Configuring LAN Settings” on page 23, select the **Keep Default IP** checkbox.
3. Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring LAN Settings

If you selected “Router” as the AP mode (see “Configuring Basic System Settings” on page 19), the LAN Settings section appears at the bottom of the Basic Settings screen.

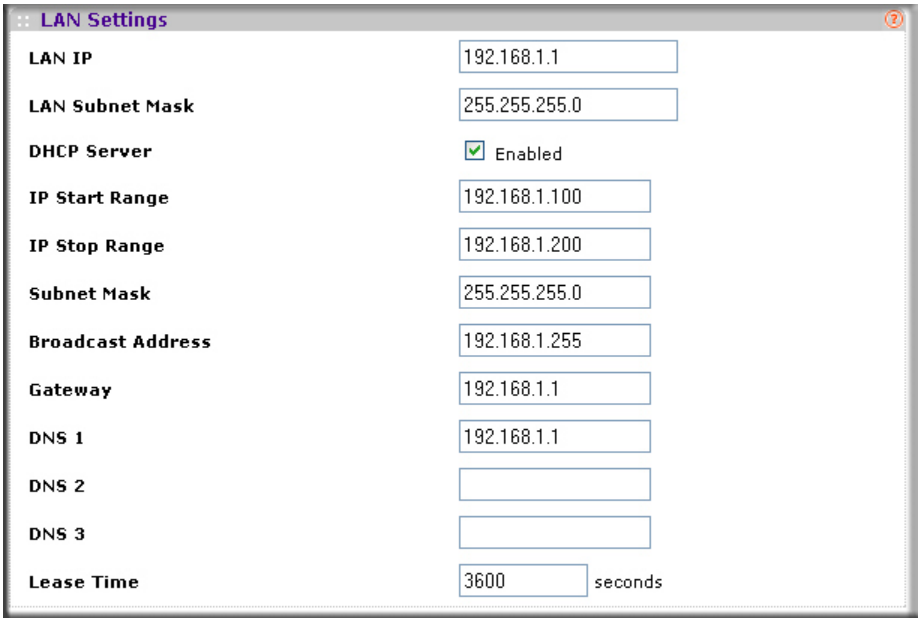


Figure 2-9

To configure the LAN settings:

1. Specify the fields as explained in *Table 2-4*, or use the default values, which work for most users and situations.

Table 2-4. LAN Settings

Field	Description
LAN IP	The LAN IP address of the wireless access point.
LAN Subnet Mask	The LAN subnet mask of the wireless access point. Combined with the LAN IP address, the LAN subnet mask enables a device to determine which other addresses are local to it, and which must be reached through a gateway.

Table 2-4. LAN Settings (continued)

Field	Description	
DHCP Server	The wireless access point is set up by default to function as a DHCP server, which provides TCP/IP configuration for computers that are connected to it. You can either use the default settings or specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the wireless access point's LAN IP address. Select the **DHCP Server** checkbox to enable the DHCP server. The screen expands, enabling you to configure the following DHCP server fields.	
	IP Start Range	The first address in the range of IP addresses to be assigned to DHCP clients. The default address is 192.168.1.100.
	IP Stop Range	The last address in the range of IP addresses to be assigned to DHCP clients. The default address is 192.168.1.200.
	Subnet Mask	The subnet mask to be used by DHCP clients. The default mask is 255.255.255.0.
	Broadcast Address	The broadcast IP address to be used by DHCP clients. The default address is 192.168.1.255.
	Gateway	The IP address of the default routing gateway to be used by DHCP clients. The default address is 192.168.1.1.
	DNS 1	The IP address of the primary static Domain Name Server (DNS) server available to DHCP clients. The default address is 192.168.1.1.
	DNS 2	The IP address of the secondary static DNS server available to DHCP clients.This server is used when the primary DNS server is not available.
	DNS 3	The IP address of the tertiary static DNS server available to DHCP clients. This server is used when the primary and secondary DNS servers are not available.
	Lease Time	The period that the DHCP server grants to the DHCP clients to use the assigned IP addresses. The default time is 3600 seconds (1 hour).

2. Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring Basic Wireless Settings

For proper compliance and compatibility between similar products in your area, you must correctly configure 802.11b/g wireless adapter settings, including the operating channel and country. The basic wireless network settings must be set correctly for wireless devices to connect to your network. For other wireless features, including wireless security, see *Chapter 3*."

WARNING!

If you configure the wireless access point from a wireless computer and you change the wireless access point's SSID, channel, or wireless security settings, you will lose your wireless connection when you click Save to Flash and Activate. You must then change the wireless settings of your computer to match the wireless access point's new settings.

Configuring 802.11b/g Wireless Settings

To configure the 802.11b/g wireless settings:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **System** > **802.11b/g Profile**. The 802.11b/g Profile screen displays.

Figure 2-10

3. Specify the 802.11n profile fields as explained *Table 2-5*.

Table 2-5. 802.11b/g Profile Settings

Field	Descriptions
Radio Enable	The radio is enabled by default. To turn off the radio, deselect the **Radio Enable** checkbox. Doing so disables access through the wireless access point, which can be helpful for configuration, network tuning, or troubleshooting activities.
Radio Policy	Select one of the following modes from the pull-down menu: • **802.11b/g**. The wireless access point accepts both 802.11b and 802.11g client association requests. This mode is also referred to as Mixed Mode. • **802.11b Only**. The wireless access point accepts 802.11b client association requests only. • **802.11g Only**. The wireless access point accepts 802.11g client association requests only.
Country	This pull-down menu lets you specify your country/region.
RF Channel	This pull-down menu lets you to specify the 802.11 channel. The available options for 802.11b or 802.11g are from 1 to 11 for the U.S. (which is the default setting) and from 1 to 13 for Europe. For automatic channel selection, select **Auto**. For more information about operating frequencies, see the guidelines about channels below this table.
Tx Output Power	This pull-down menu lets you to specify the transmission power. The available options are from 27 dBm to 18 dBm. By default, the Tx Output Power is 27 dBm. **Note**: Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country.

You should not need to change the operating frequency (channel) unless you notice interference problems, or are setting up the wireless access point near another wireless access point. Observe the following guidelines:

- Wireless access points use a fixed channel. You can select a channel that provides the least interference and best performance. In the USA and Canada, 11 channels are available.
- If using multiple wireless access points, it is better if adjacent wireless access points use different channels to reduce interference. The recommended channel spacing between adjacent wireless access points is five channels (for example, use channels 1 and 6, or 6 and 11).
- In “infrastructure” mode, wireless stations normally scan all channels, looking for a wireless access point. If more than one wireless access point can be used, the one with the strongest signal is used. This can happen only when the wireless access points use the same SSID. The WGAP150 wireless access point functions in “infrastructure” mode by default.

For more information about wireless channels, see the online document that you can access from “Wireless Networking Basics” in Appendix B.

4. Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring Basic Wireless Network Settings

To configure the basic wireless network settings:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **Wireless Networks**. The Wireless Networks screen displays.

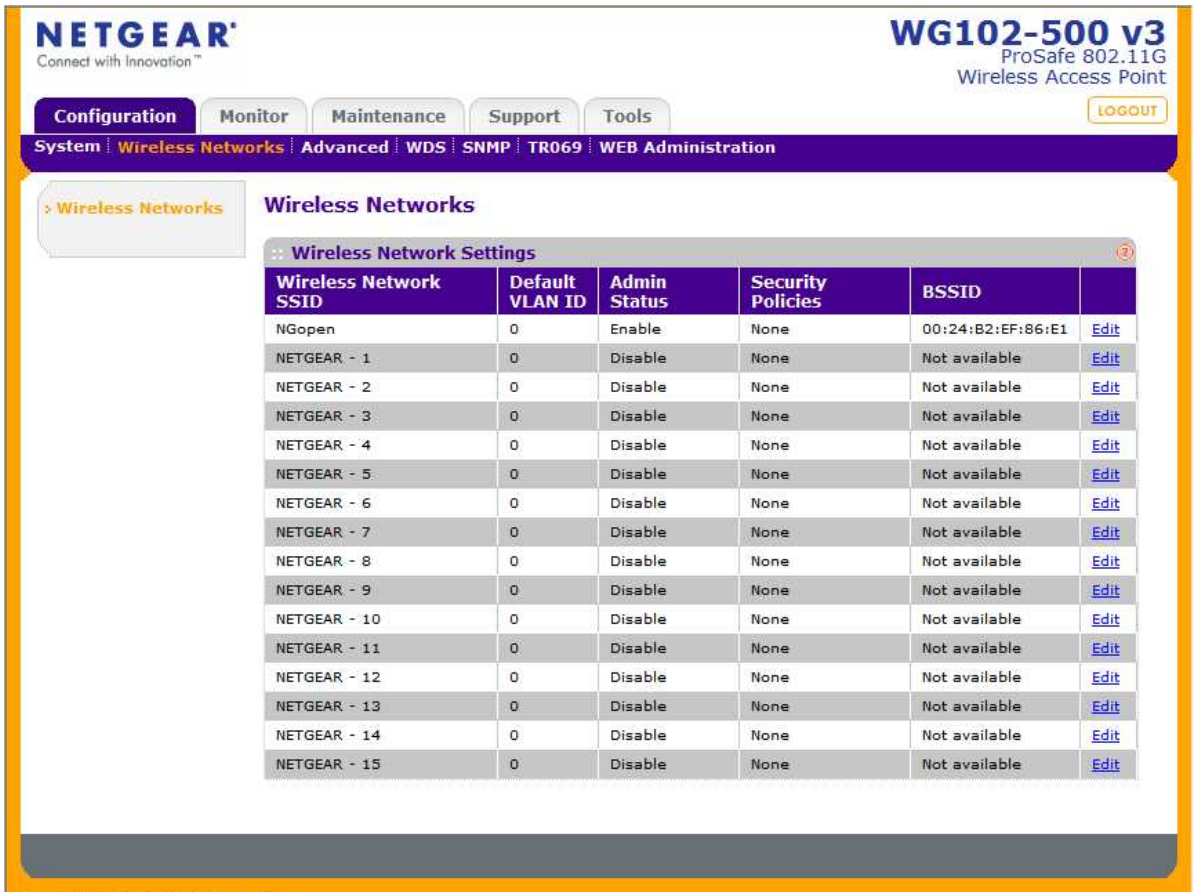

NETGEAR
Connect with Innovation™
WG102-500 v3
ProSafe 802.11G
Wireless Access Point
Configuration
Monitor
Maintenance
Support
Tools
LOGOUT
System
Wireless Networks
Advanced
WDS
SNMP
TR069
WEB Administration
Wireless Networks
Wireless Networks
Wireless Network Settings
Wireless Network SSID
Default VLAN ID
Admin Status
Security Policies
BSSID
NGopen 0 Enable None 00:24:B2:EF:86:E1 Edit
NETGEAR - 1 0 Disable None Not available Edit
NETGEAR - 2 0 Disable None Not available Edit
NETGEAR - 3 0 Disable None Not available Edit
NETGEAR - 4 0 Disable None Not available Edit
NETGEAR - 5 0 Disable None Not available Edit
NETGEAR - 6 0 Disable None Not available Edit
NETGEAR - 7 0 Disable None Not available Edit
NETGEAR - 8 0 Disable None Not available Edit
NETGEAR - 9 0 Disable None Not available Edit
NETGEAR - 10 0 Disable None Not available Edit
NETGEAR - 11 0 Disable None Not available Edit
NETGEAR - 12 0 Disable None Not available Edit
NETGEAR - 13 0 Disable None Not available Edit
NETGEAR - 14 0 Disable None Not available Edit
NETGEAR - 15 0 Disable None Not available Edit

Figure 2-11

Table 2-6 on page 27 explains the fields of the Wireless Network Settings table.

Table 2-6. Wireless Network Settings

Field	Description
Wireless Network SSID	The wireless network name (SSID) for the wireless security profile.
Default VLAN ID	The default VLAN ID that is associated with the wireless security profile.
Admin Status	The status of the wireless security profile (Enabled or Disabled).

Table 2-6. Wireless Network Settings (continued)

Field	Description
Security Policies	The configured wireless authentication and encryption methods for the wireless security profile.
BSSID	The detailed BSSID for the wireless security profile. This BSSID consist of the MAC address of the wireless access point with the last digit altered. If the MAC address ends with F0, the BSSID for the first profile ends with F1, for the second profile with F2, for the third profile with F3, and so on.
Edit (hyperlink)	The hyperlink to the Edit Wireless Network screen with the configurable fields for the wireless security profile.

3. Click the Edit hyperlink of the first wireless security profile (NETGEAR - 0). The Edit Wireless Network screen opens for the first wireless security profile.

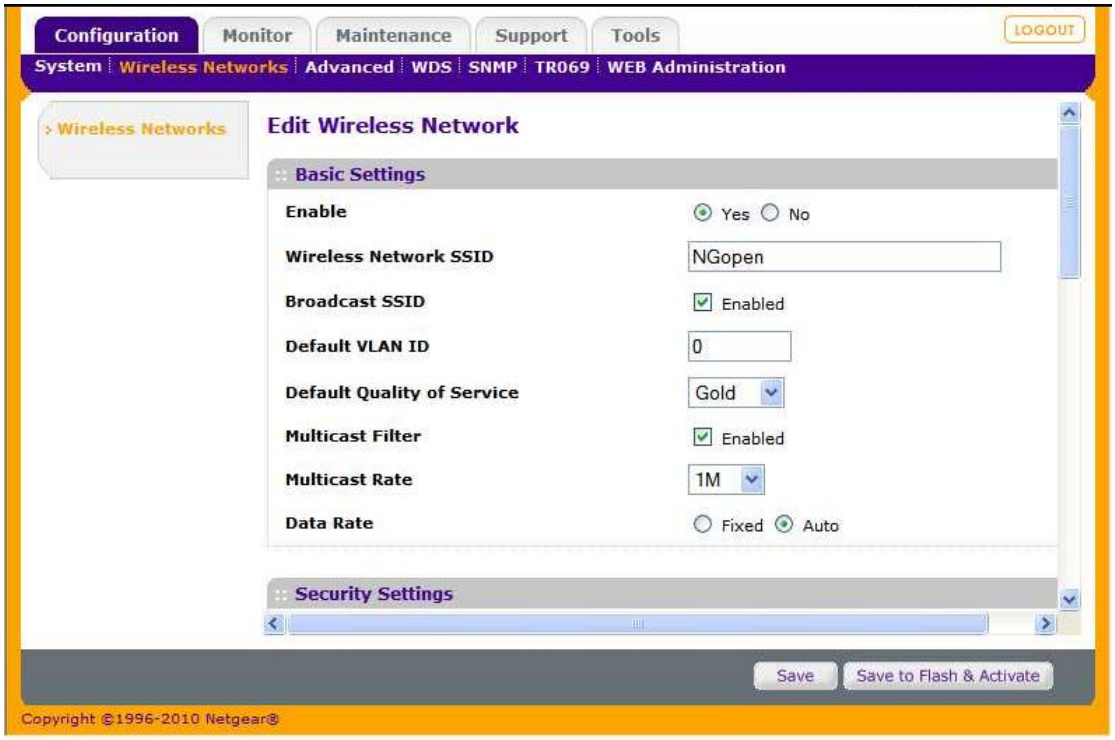


Figure 2-12

4. In the Basic Settings section of the Edit Wireless Network screen, specify the fields as explained in *Table 2-7*.

Table 2-7. Wireless Network Settings

Field	Description
Enable	Select one of the following options: • **Yes**. Select this radio button to enable the wireless security profile. This is the default setting. • **No**. Select this radio button to disable the wireless security profile.
Wireless Network SSID	The SSID is also known as the wireless network name. The SSID separates network traffic from different wireless networks. To connect any wireless device to a wireless network, you need to use the SSID. The wireless access point default SSIDs are: NETGEAR_0 for the first profile, NETGEAR_1 for the second profile, NETGEAR_2 for the third profile, and so on. You can enter a value of up to 32 alphanumeric characters. For more information about SSIDs, see "Security Profiles" on page 35. **Note**: The SSID of any wireless adapters must match the SSID of the wireless access point. If they do not match, a wireless connection to the wireless access point cannot be established.
Broadcast SSID	Select the **Broadcast SSID** checkbox to enable broadcast of the SSID. If you disable broadcast of the SSID, only stations that know the SSID can connect to the wireless access point. Disabling the SSID broadcast somewhat hampers the wireless network discovery feature of some products. Broadcast of the SSID is enabled by default.
Default VLAN ID	Specify the default VLAN ID that is associated with the wireless security profile and that will be tagged on all egress packets. The default VLAN can be active only when the wireless access point functions as a bridge (for more information, see "Configuring Basic System Settings" on page 19). **Note**: The default VLAN ID can be specified in an authentication reply from the RADIUS server. However, if a per-user VLAN ID is specified in the authentication reply from the RADIUS server, the value that is specified in default VLAN ID will be overridden.
Default Quality of Service	Select one of the following Quality of Service (QoS) options from the pull-down menu: • **Gold**. Wireless traffic is sent with a best-effort priority. For example, you could assign this level to voice and video traffic. • **Silver**. Wireless traffic is sent in the background. For example, you could assign this level to regular data traffic. • **Bronze**. Wireless traffic is sent with the lowest priority ("spare"). For example, you could assign this level to FTP traffic.

Table 2-7. Wireless Network Settings (continued)

Field	Description
Multicast Filter	Select the **Multicast Filter** checkbox to enable filtering of egress multicast packets that are sent from the wireless access point.
Multicast Rate	Select the data rate for egress multicast packets from the pull-down menu. The smallest data rate that you can select is 1 Mbps; the largest is 54 Mbps. The default rate is 1 Mbps.
Data Rate	Select one of the following options: • **Fixed**. All data packets are transmitted according to the transmit rate that you select from the pull-down menu. The smallest data rate that you can select is 1 Mbps; the largest is 54 Mbps. The default rate is 1 Mbps. • **Auto**. All data packets are transmitted according to the automatically selected best transmit rate.

5. Click **Save** or **Save to Flash & Activate** to save your settings.

Note: Other wireless settings on the Edit Wireless Network screen are discussed in Chapter 3, “Wireless Configuration and Security.”

Testing Basic Wireless Connectivity

After you configured the wireless access point as explained in the previous section, test your computers for wireless connectivity before you position and mount the wireless access point at its permanent position:

1. 1. Configure the 802.11b/g or 802.11n wireless adapters of your computers so that they all have the same SSID and channel that you have configured on the wireless access point.
2. 2. Verify that your computers have a wireless link to the wireless access point and are able to obtain an IP address through DHCP from the wireless access point.
3. 3. Verify network connectivity by using a browser such as Internet Explorer 6.0 or above, or Mozilla Firefox 1.5 or above to browse the Internet, or check for file and printer access on your network.

Note: If you have trouble connecting to the wireless access point, see Chapter 6.

WARNING!

Before you deploy the wireless access point in your network, set up wireless security and other wireless features as described in Chapter 3.

In addition to wireless security and other wireless features, before you deploy the wireless access point in your network, configure any additional features as described in Chapter 4 and Chapter 5. After you have completed the configuration of the wireless access point, you can reconfigure the computer that you used for this process back to its original TCP/IP settings.

3 Wireless Configuration and Security

This chapter describes how to configure the wireless features of your wireless access point. In planning your wireless network, consider the level of security required.

WARNING!

If you are configuring the wireless access point from a wireless PC and you change the wireless access point's SSID, channel, or wireless security settings, you will lose your wireless connection when you click Apply. You must then change the wireless settings of your PC to match the wireless access point's new settings.

Before you set up wireless security and additional wireless features that are described in this chapter, connect the wireless access point, get the Internet connection working, configure 802.11b/g wireless settings, and configure basic wireless network settings, as described in *Chapter 2*. The wireless access point should work with an Ethernet LAN connection and wireless connectivity should have been verified before you set up wireless security and additional wireless features.

This chapter includes:

- *Wireless Data Security Options* on this page
- "Security Profiles" on page 35
- "Configuring RADIUS Server Settings" on page 45
- "WAPI Certificates" on page 49
- "Configuring Alternate DHCP Server Settings" on page 52
- "Configuring Wireless Quality of Service" on page 54
- "Configuring Wireless Client Separation" on page 58

Wireless Data Security Options

Indoors, computers can connect over 802.11n wireless networks at a maximum range of 300 feet. Typically, a wireless access point inside a building works best with devices within a 100

foot radius. Such distances can allow for others outside your immediate area to access your network.

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The wireless access point provides highly effective security features that are covered in detail in this chapter. Deploy the security features appropriate to your needs.

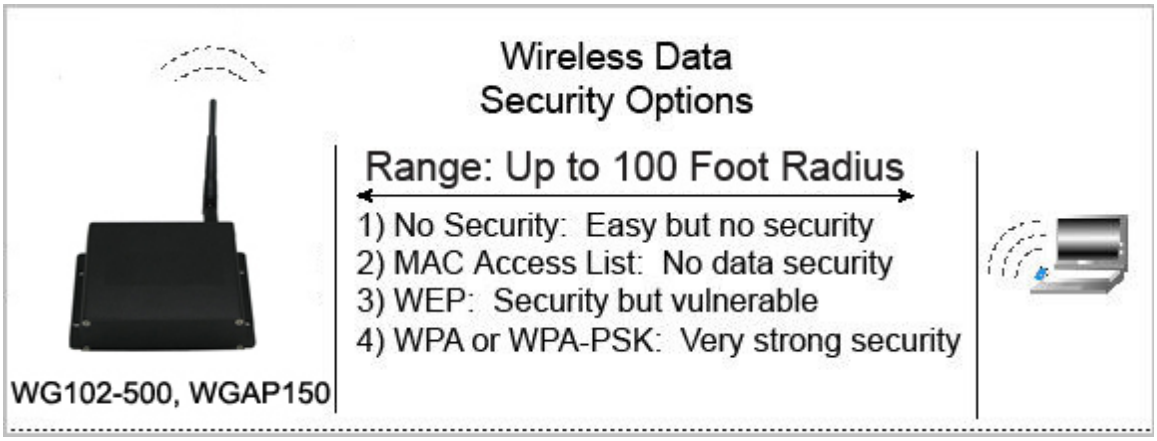

Wireless Data
Security Options
Range: Up to 100 Foot Radius
1) No Security: Easy but no security
2) MAC Access List: No data security
3) WEP: Security but vulnerable
4) WPA or WPA-PSK: Very strong security
WG102-500, WGAP150

Figure 3-1

Note: *Figure 3-1* shows the WGAP150 with an external antenna, which does not come standard with the product.

There are several ways you can enhance the security of your wireless network:

- **Use Multiple BSSIDs combined with VLANs**. You can configure combinations of VLANS and BSSIDs with stronger or less restrictive access security according to your requirements. For example, visitors could be given wireless Internet access but be excluded from any access to your internal network. For information about how to configure BSSIDs, see “Creating and Editing Security Profiles” on page 37.
- **Restrict Access based by MAC address**. You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the wireless access point. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. For information about how to restrict access by MAC address, see “WAPI Certificates” on page 49.
- **Turn off the broadcast of the wireless network name (SSID)**. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network discovery feature of some products, such as Windows XP, but the data is still exposed. For information about how to turn of broadcast of the SSID, see “Creating and Editing Security Profiles” on page 37.

- **WEP**. Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK. For information about how to configure static and dynamic WEP, see "Configuring Static WEP" on page 40 and "Configuring Legacy 802.1X (or Dynamic WEP)" on page 41.
- **WPA and WPA-PSK (TKIP)**. Wi-Fi Protected Access (WPA) data encryption provides strong data security with Temporal Key Integrity Protocol (TKIP) encryption. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. WPA uses RADIUS-based 802.1x authentication; WPA-PSK uses a pre-shared key (PSK) for authentication. For information about how to configure WPA, see "Configuring WPA and WPA-PSK (TKIP)" on page 41.
- **WPA2 and WPA2-PSK (AES)**. Wi-Fi Protected Access version 2 (WPA2) data encryption provides strong data security with Advanced Encryption Standard (AES) encryption. The very strong authentication along with dynamic per frame rekeying of WPA2 make it virtually impossible to compromise. WPA2 uses RADIUS-based 802.1x authentication; WPA2-PSK uses a pre-shared key (PSK) for authentication. For information about how to configure WPA2, see "Configuring WPA2 and WPA2-PSK (AES)" on page 43.
- **WPA+WPA2 and WPA-PSK+WPA2-PSK Mixed Modes**. These modes support data encryption either with both WPA and WPA2 clients or with both WPA-PSK and WPA2-PSK clients and provide the most reliable security. For information about how to configure WPA+WPA2 and WPA-PSK+WPA2-PSK, see "Configuring WPA+WPA2 and WPA-PSK+WPA2-PSK Mixed Modes" on page 44.

Security Profiles

Security profiles let you configure unique security settings for each SSID. The wireless access point supports up to 16 BSSIDs that you can configure in the individual Edit Wireless Network screens that are accessible from the Wireless Networks screen (see "Creating and Editing Security Profiles" on page 37).

To set up a security profile you select its network authentication type, data encryption, wireless client security separation, and VLAN ID:

- Network Authentication
  The wireless access point is set by default as an open system with no authentication. When you configure network authentication, bear in mind that not all wireless adapters support WPA or WPA2. Windows XP, Windows 2000 with Service Pack 3, and Windows Vista do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions on configuring WPA2 settings.

  For information about the types of network authentication that the wireless access point supports, see "Creating and Editing Security Profiles" on page 37.
- Data Encryption
  Select the data encryption that you want to use. The available options depend on the

network authentication setting above (otherwise, the default is None). The data encryption settings are explained in “Creating and Editing Security Profiles” on page 37.

- Wireless Client Security Separation
  If enabled, the associated wireless clients (using the same SSID) will not be able to communicate with each other. This feature is useful for hotspots and other public access situations. By default, wireless client separation is disabled. For more information, see “Configuring Wireless Client Separation” on page 58.
- VLAN ID
  If enabled and if the network devices (hubs and switches) on your LAN support the VLAN (802.1Q) standard, the default VLAN ID for the wireless access point will be associated with each profile. The default VLAN ID must match the IDs that are used by the other network devices. This feature is available only when the AP Mode is set to Bridge (see “Configuring Basic Wireless Network Settings” on page 27).

Some concepts and guidelines regarding the SSID are explained below:

- A Basic Service Set (BSS) is a group of wireless stations and a single wireless access point, all using the same SSID.
- An Extended Service Set (ESS) is a group of wireless stations and multiple wireless access points, all using the same ID (ESSID).
- Different wireless access points within an ESS can use different channels. To reduce interference, adjacent wireless access points should use different channels.
- Roaming is the ability of wireless stations to connect wirelessly when they physically move from one BSS to another within the same ESS. The wireless station automatically changes to the wireless access point with the least interference or best performance.

Before You Change the SSID, WEP, and WPA Settings

For a new wireless network, print or copy this form and fill in the settings. For an existing wireless network, the network administrator can provide this information. Be sure to set the Country/Region correctly as the first step. Store this information in a safe place.

- **SSID*:*** The Service Set Identification (SSID) identifies the wireless local area network. You may customize it by using up to 32 alphanumeric characters. Write your SSID on the line.

  SSID: _____

> **Note:** The SSID in the wireless access point is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID:

- **WEP Key Size, Key Format Passphrase, and Authentication**
  Choose the key size by circling one: 64, 128, or 152 bits.

Choose the key format by circling one: ASCII or HEX.
Choose the authentication type by circling one: Open or Shared.

Passphrase: _____

Note: If you select shared key, the other devices in the network will not connect unless they are set to shared key and have the same keys in the same positions as those in the wireless access point.

- **WPA-PSK (Pre-Shared Key), WPA2-PSK (Pre-Shared Key)**
  Record the WPA-PSK passphrase: Record the WPA2-PSK passphrase:

  WPA-PSK Passphrase: _____

  WPA2-PSK Passphrase: _____

- **WPA RADIUS Settings**
  For WPA, record the following settings for the primary and secondary RADIUS servers:

  Server Name/IP Address: Primary _____ Secondary _____

  Port: _____

  Shared Secret: _____

- **WPA2 RADIUS Settings**
  For WPA2, record the following settings for the primary and secondary RADIUS servers:

  Server Name/IP Address: Primary _____ Secondary _____

  Port: _____

  Shared Secret: _____

Creating and Editing Security Profiles

To create or edit a security profile with its own unique BSSID:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.

2. Select **Configuration** > **Wireless Networks**. The Wireless Networks screen opens, displaying 16 wireless security profiles.

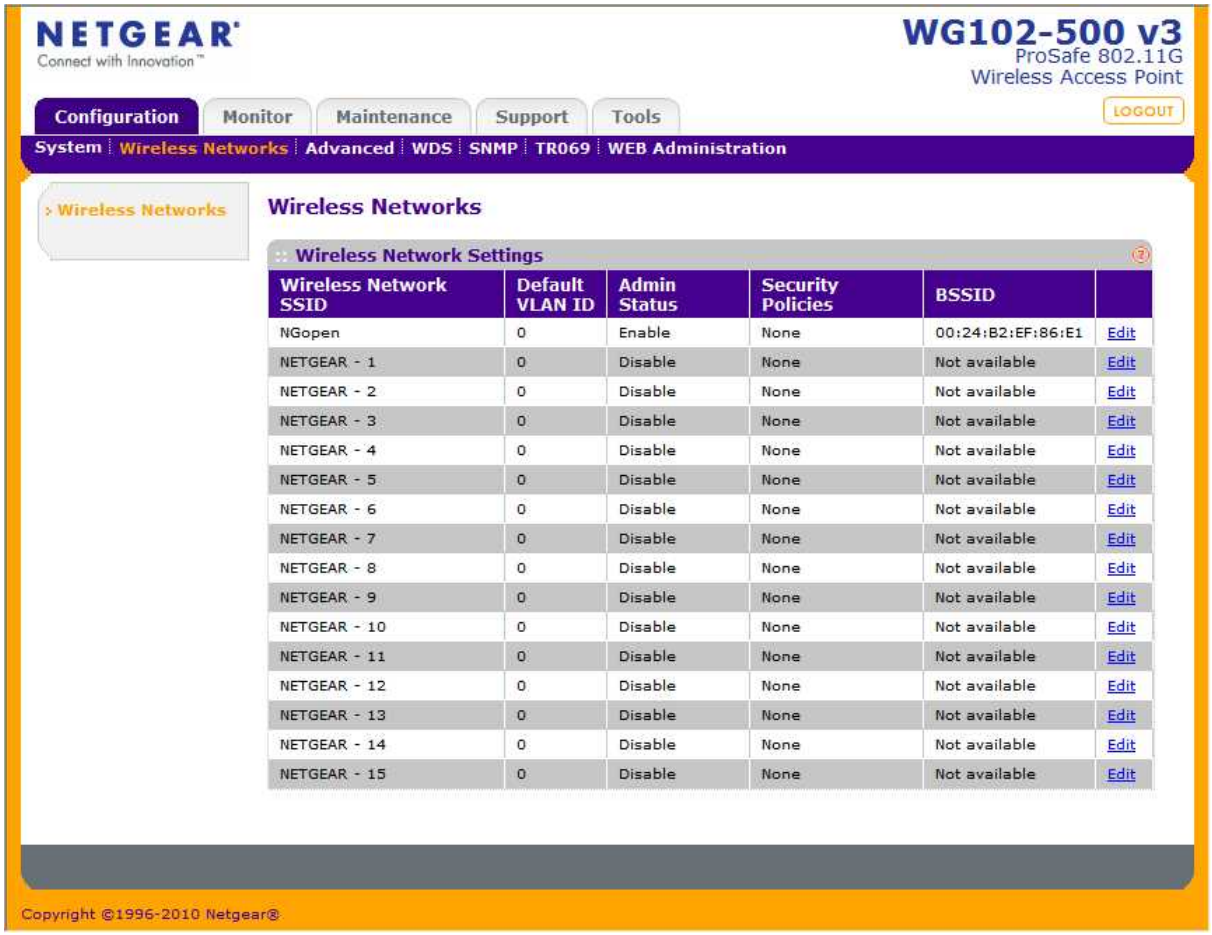

NETGEAR
Connect with Innovation™
WG102-500 v3
ProSafe 802.11G
Wireless Access Point
Configuration
Monitor
Maintenance
Support
Tools
LOGOUT
System
Wireless Networks
Advanced
WDS
SNMP
TR069
WEB Administration
Wireless Networks
Wireless Networks
Wireless Network Settings
Wireless Network SSID
Default VLAN ID
Admin Status
Security Policies
BSSID
NGopen 0 Enable None 00:24:B2:EF:86:E1 Edit
NETGEAR - 1 0 Disable None Not available Edit
NETGEAR - 2 0 Disable None Not available Edit
NETGEAR - 3 0 Disable None Not available Edit
NETGEAR - 4 0 Disable None Not available Edit
NETGEAR - 5 0 Disable None Not available Edit
NETGEAR - 6 0 Disable None Not available Edit
NETGEAR - 7 0 Disable None Not available Edit
NETGEAR - 8 0 Disable None Not available Edit
NETGEAR - 9 0 Disable None Not available Edit
NETGEAR - 10 0 Disable None Not available Edit
NETGEAR - 11 0 Disable None Not available Edit
NETGEAR - 12 0 Disable None Not available Edit
NETGEAR - 13 0 Disable None Not available Edit
NETGEAR - 14 0 Disable None Not available Edit
NETGEAR - 15 0 Disable None Not available Edit
Copyright ©1996-2010 Netgear®

Figure 3-2

Table 3-1 explains the fields of the Wireless Network Settings table.

Table 3-1. Wireless Network Settings

Field	Description
Wireless Network SSID	The wireless network name (SSID) for the wireless security profile.
Default VLAN ID	The default VLAN ID that is associated with the wireless security profile.
Admin Status	The status of the wireless security profile (Enabled or Disabled).
Security Policies	The configured wireless authentication and encryption methods for the wireless security profile.

Table 3-1. Wireless Network Settings (continued)

Field	Description
BSSID	The detailed BSSID for the wireless security profile. This BSSID consist of the MAC address of the wireless access point with the last digit altered. If the MAC address ends with F0, the BSSID for the first profile ends with F1, for the second profile with F2, for the thirds profile with F3, and so on.
Edit (hyperlink)	The hyperlink to the Edit Wireless Network screen with the configurable fields for the wireless security profile.

3. To configure or edit a wireless security profile, select the corresponding Edit hyperlink to the right of the wireless security profile. The Edit Wireless Network screen opens for the selected wireless security profile. The first section on the screen is the Basic Settings section. "Configuring Basic Wireless Network Settings" on page 27 explains the fields in this section. Scroll down to the Security Settings section.

Figure 3-3

4. Select one of the following security options from the Security Policy pull-down menu:
   - **None**. No security is the default settings.
   - **Static WEP**. See "Configuring Static WEP" on page 40.
   - **802.1X**. See "Configuring Legacy 802.1X (or Dynamic WEP)" on page 41.
   - **WPA-TKIP**. See "Configuring WPA and WPA-PSK (TKIP)" on page 41.
   - **WPA2-AES**. See "Configuring WPA2 and WPA2-PSK (AES)" on page 43.
   - **WPA-TKIP and WPA2-AES**. See "Configuring WPA+WPA2 and WPA-PSK+WPA2-PSK Mixed Modes" on page 44.
5. Click **Save** or **Save to Flash & Activate** to save your settings.

Note: If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Save to Flash and Activate. Reconfigure your wireless computer to match the new settings, or access the wireless access point from a wired computer to make further changes.

For more information about wireless security options, see the online document that you can access from "Wireless Networking Basics" in Appendix B.

Configuring Static WEP

Static WEP provides pre-shared WEP key encryption without (RADIUS) authentication. The security level of static WEP is not very strong.When you select Static WEP from the Security Policy pull-down menu, the section expands to display the static WEP fields.

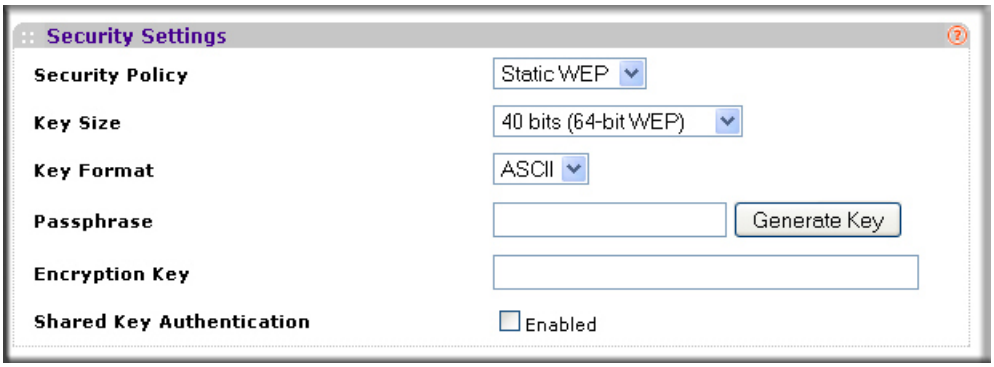


Figure 3-4

Specify the fields that are explained in *Table 3-2*.

Table 3-2.

Field	Descriptions
Key Size	This pull-down menu lets you select the encryption key size: • **40 bits (64-bit WEP)** • **104 bits (128-bit WEP)** • **128 bits (152-bit WEP)**
Key Format	This pull-down menu lets you select the encryption key format: • **ASCII**. The ASCII format applies only to encryption keys that are manually entered. • **HEX**. The HEX format applies both to keys that are manually entered and that are automatically generated. **Note**: For automatic encryption key generation, the strongest encryption is provided by a combination of a key with 128-bits and the HEX key format.
Passphrase	Enter a passphrase. The passphrase length must be between 8 and 63 characters (inclusive). To generate an encryption key, click **Generate Key**.
Encryption Key	Either manually enter a key or allow the key to be automatically generated by clicking **Generate Key**. • For ASCII format, depending on the key size selected, the manually entered encryption key must have a length of 5, 13, or 16 characters. • For HEX format, depending on the key size selected, the manually entered or automatically generated encryption key must have a length of 10, 26, or 32 characters. Wireless stations must use the key to access the wireless access point. **Note**: Not all wireless adapters support passphrase key generation.

Table 3-2.

Field	Descriptions
Shared Key Authentication	The default authentication setting is Open System authentication. Select the **Shared Key Authentication** checkbox to enable shared key authentication. **Note**: The authentication method is separate from the data encryption. You can select an authentication method that requires a shared key but still leaves the data transmissions unencrypted. If you require strong security, use both the Shared Key and WEP encryption settings.

Configuring Legacy 802.1X (or Dynamic WEP)

To use legacy 802.1X security, you also must define RADIUS server settings. For information about RADIUS servers, see "Configuring RADIUS Server Settings" on page 45.

When you select 802.1X from the Security Policy pull-down menu, the section expands to display the 802.1X fields.

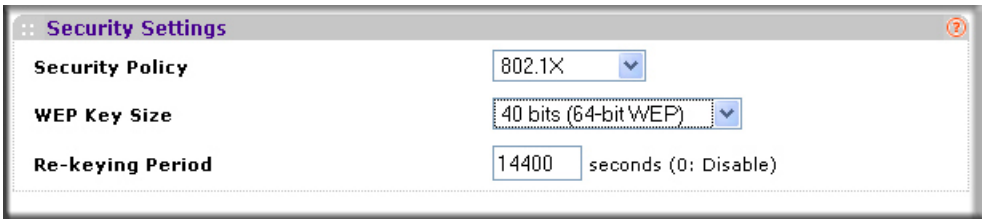


Figure 3-5

Specify the fields that are explained in *Table 3-3*.

Table 3-3.

Field	Descriptions
WEP Key Size	This pull-down menu lets you select the encryption key size: • **40 bits (64-bit WEP)** • **104 bits (128-bit WEP)**
Rekeying Period	The period during which the broadcast key remains valid. When the period expires, the broadcast key is no longer valid and must be renewed. The default is 14400 seconds (4 hours). To disable re-keying, enter a value of 0.

Configuring WPA and WPA-PSK (TKIP)

WPA security requires RADIUS-based 802.1x authentication, so you also must define RADIUS server settings. For information about RADIUS servers, see "Configuring RADIUS Server Settings" on page 45. WPA-PSK security uses a pre-shared key (PSK) and does not require authentication from a RADIUS server. Both methods use Temporal Key Integrity Protocol (TKIP) encryption.

When you select WPA-TKIP from the Security Policy pull-down menu, the section expands to display the WPA-TKIP fields. *Figure 3-6* shows Pre-Shared Key user authentication as an example.

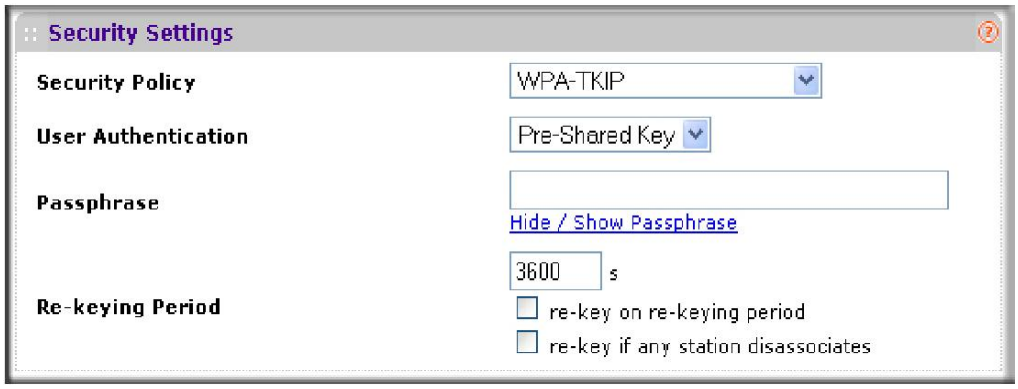


Figure 3-6

Specify the fields that are explained in *Table 3-4*.

Table 3-4.

Field	Descriptions		
User Authentication	Pre-Shared Key	From the User Authentication pull-down menu, select the **Pre-Shared Key** to enable WPA-PSK. WPA-PSK does not require a RADIUS server for authentication, but you must specify a passphrase.	
		Passphrase	Enter a passphrase with a length must between 8 and 63 characters (inclusive). Click the **Hide / Show Passphrase** hyperlink to switch between hiding and showing the passphrase on screen. Hiding the passphrase provides added security in a public environment.
	RADIUS	From the User Authentication pull-down menu, select **RADIUS** to enable WPA, which requires a RADIUS server for authentication (see "Configuring RADIUS Server Settings" on page 45). This is the default user authentication setting.	
Re-Keying Period	The period during which the broadcast key remains valid. When the period expires, the broadcast key is no longer valid and must be renewed. The default is 3600 seconds (1 hour).		
Re-key on re-keying period	Select the **Re-key on re-keying period** checkbox to require rekeying after the rekeying period has expired.		
Re-key if any station disassociates	Select the **Re-key if any station disassociates** checkbox to require rekeying after any wireless station logs off from the wireless access point.		

Configuring WPA2 and WPA2-PSK (AES)

WPA2 security requires RADIUS-based 802.1x authentication, so you also must define RADIUS server settings. For information about RADIUS servers, see "Configuring RADIUS Server Settings" on page 45. WPA2-PSK security uses a pre-shared key (PSK) and does not require authentication from a RADIUS server. Both methods use Advanced Encryption Standard (AES) encryption.

When you select WPA2-AES from the Security Policy pull-down menu, the section expands to display the WPA2-AES fields. Figure 3-7 on page 43 shows RADIUS user authentication as an example.

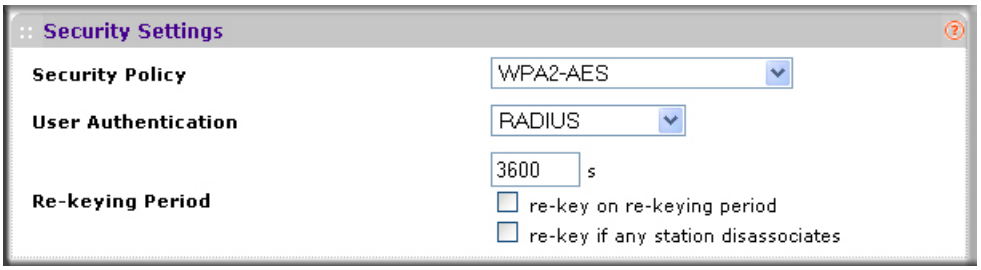


Figure 3-7

Specify the fields that are explained in *Table 3-5*.

Table 3-5.

Field	Descriptions		
User Authentication	Pre-Shared Key	From the User Authentication pull-down menu, select the **Pre-Shared Key** to enable WPA2-PSK. WPA2-PSK does not require a RADIUS server for authentication, but you must specify a passphrase.	
		Passphrase	Enter a passphrase with a length must between 8 and 63 characters (inclusive). Click the **Hide / Show Passphrase** hyperlink to switch between hiding and showing the passphrase on screen. Hiding the passphrase provides added security in a public environment.
	RADIUS	From the User Authentication pull-down menu, select **RADIUS** to enable WPA2, which requires a RADIUS server for authentication (see "Configuring RADIUS Server Settings" on page 45). This is the default user authentication setting.	
Re-Keying Period	The period during which the broadcast key remains valid. When the period expires, the broadcast key is no longer valid and must be renewed. The default is 3600 seconds (1 hour).		
Re-key on re-keying period	Select the **Re-key on re-keying period** checkbox to require rekeying after the rekeying period has expired.		
Re-key if any station disassociates	Select the **Re-key if any station disassociates** checkbox to require rekeying after any wireless station logs off from the wireless access point.		

Configuring WPA+WPA2 and WPA-PSK+WPA2-PSK Mixed Modes

WPA+WPA2 security requires RADIUS-based 802.1x authentication, so you also must define RADIUS server settings. For information about RADIUS servers, see "Configuring RADIUS Server Settings" on page 45. WPA-PSK+WPA2-PSK security uses a pre-shared key (PSK) and does not require authentication from a RADIUS server. Depending on the wireless client, these mixed modes use either TKIP or AES encryption.

When you select WPA-TKIP and WPA2-AES from the Security Policy pull-down menu, the section expands to display the WPA-TKIP and WPA2-AES fields. *Figure 3-8* shows Pre-Shared Key user authentication as an example.

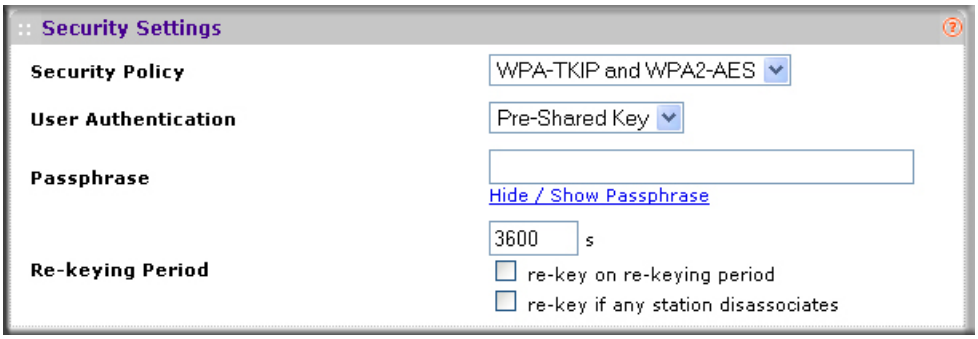


Figure 3-8

Specify the fields that are explained in *Table 3-6*.

Table 3-6.

Field	Descriptions		
User Authentication	Pre-Shared Key	From the User Authentication pull-down menu, select the **Pre-Shared Key** to enable WPA-PSK+WPA2-PSK. This mixed mode does not require a RADIUS server for authentication, but you must specify a passphrase.	
		Passphrase	Enter a passphrase with a length must between 8 and 63 characters (inclusive). Click the **Hide / Show Passphrase** hyperlink to switch between hiding and showing the passphrase on screen. Hiding the passphrase provides added security in a public environment.
	RADIUS	From the User Authentication pull-down menu, select **RADIUS** to enable WPA+WPA2, which requires a RADIUS server for authentication (see "Configuring RADIUS Server Settings" on page 45). This is the default user authentication setting.	
Re-Keying Period	The period during which the broadcast key remains valid. When the period expires, the broadcast key is no longer valid and must be renewed. The default is 3600 seconds (1 hour).		
Re-key on re-keying period	Select the **Re-key on re-keying period** checkbox to require rekeying after the rekeying period has expired.		

Table 3-6.

Field	Descriptions
Re-key if any station disassociates	Select the **Re-key if any station disassociates** checkbox to require rekeying after any wireless station logs off from the wireless access point.

Configuring RADIUS Server Settings

For authentication, accounting, or both authentication and accounting using RADIUS, you must configure primary servers and optional secondary servers. The general RADIUS server settings can apply to all devices that are connected to the wireless access point. For each individual SSID, you can also configure alternate RADIUS server settings that override the general RADIUS server settings and that apply only to the devices that are connected to the SSID.

Configuring General RADIUS Server Settings

To view or change the general RADIUS server settings:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **System** > **Radius Server**. The Radius Server screen displays (see Figure 3-9 on page 46).

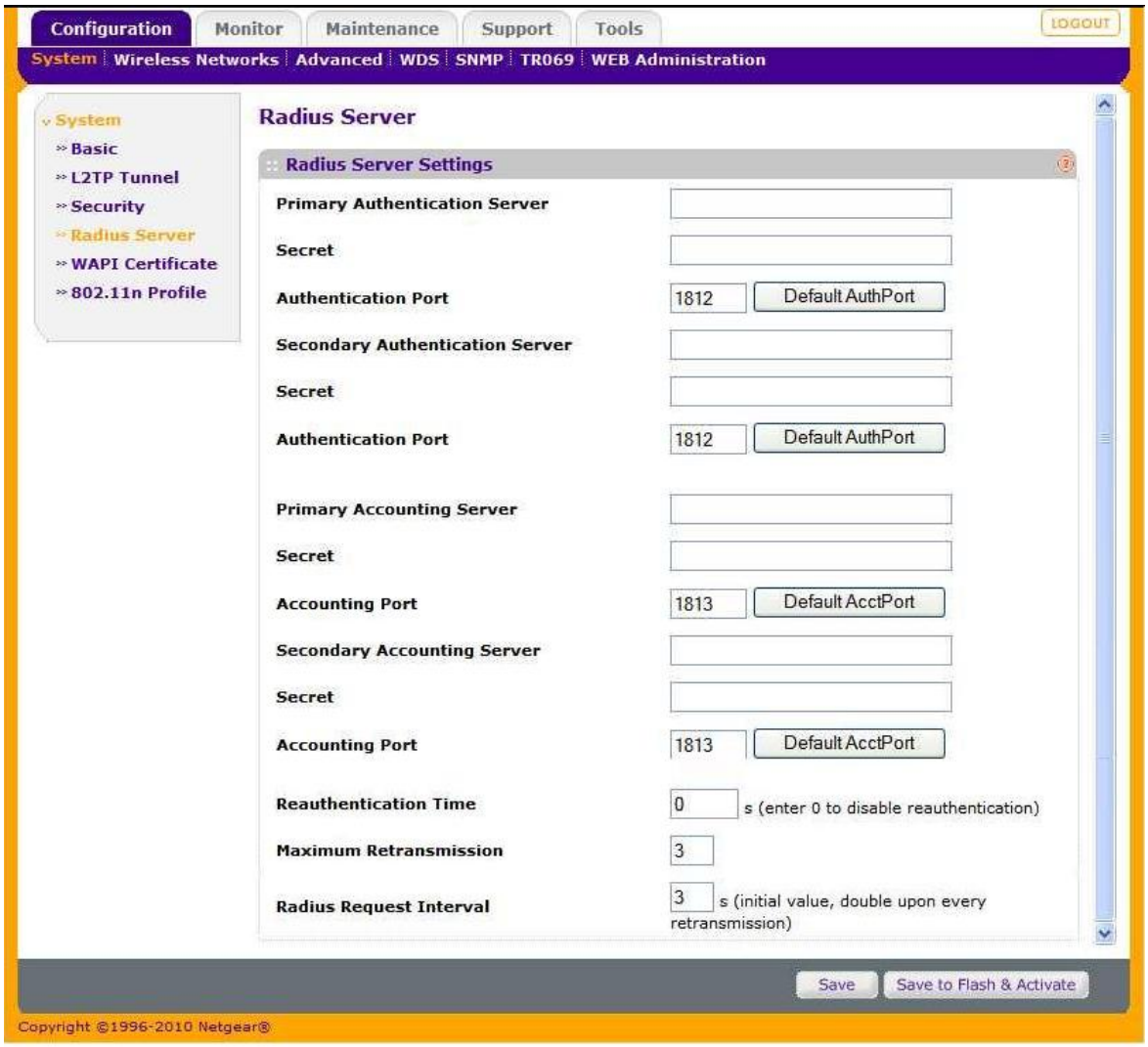


Figure 3-9

3. Specify the fields that are explained in *Table 3-7*.

Table 3-7. RADIUS Server Settings

Field	Descriptions
Primary Authentication Server	The IP address of the primary RADIUS server for authentication. The default address is 0.0.0.0.
Secret	The shared key between the wireless access point and the primary RADIUS server during authentication.
Authentication Port	The UDP port number on the wireless access point that is used to access the primary RADIUS server for authentication. Click **Default AuthPort** to revert to the default port, which is number 1812.

Table 3-7. RADIUS Server Settings (continued)

Field	Descriptions
Secondary Authentication Server	The IP address of the secondary RADIUS server for authentication. The default address is 0.0.0.0. The secondary RADIUS server is used when the primary RADIUS server is not available.
Secret	The shared key between the wireless access point and the secondary RADIUS server during authentication.
Authentication Port	The UDP port number on the wireless access point that is used to access the secondary RADIUS server for authentication. Click **Default AuthPort** to revert to the default port, which is number 1812.
Primary Accounting Server	The IP address of the primary RADIUS server for accounting. The default address is 0.0.0.0.
Secret	The shared key between the wireless access point and the primary RADIUS server during the accounting process.
Authentication Port	The UDP port number on the wireless access point that is used to access the primary RADIUS server for accounting. Click **Default AuthPort** to revert to the default port, which is number 1813.
Secondary Accounting Server	The IP address of the secondary RADIUS server for accounting. The default address is 0.0.0.0. The secondary RADIUS server is used when the primary RADIUS server is not available.
Secret	The shared key between the wireless access point and the secondary RADIUS server during the accounting process.
Authentication Port	The UDP port number on the wireless access point that is used to access the secondary RADIUS server for accounting. Click **Default AuthPort** to revert to the default port, which is number 1813.
Reauthentication Time	The time in seconds that the RADIUS request attempts should continue after the first authentication attempt. Enter 0 to disable reauthentication, which is the default setting.
Maximum Retransmission	The maximum number of RADIUS request attempts after the first authentication attempt. The default is 3 attempts.
Radius Request Interval	The interval in seconds between each RADIUS request attempt. The specified time interval is doubled for every retransmission. The default is 3 seconds.

4. Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring Alternate RADIUS Server Settings

Alternate RADIUS server settings override the general RADIUS server settings and apply only to the devices that are connected to the individual SSID for which you configure the Alternate RADIUS server settings.

To configure alternate RADIUS server settings for an individual SSID:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **Wireless Networks**. The Wireless Networks screen opens, displaying 16 wireless security profiles (see Figure 3-2 on page 38).
3. To configure or edit a wireless security profile, select the corresponding Edit hyperlink to the right of the wireless security profile. The Edit Wireless Network screen opens for the selected wireless security profile. Scroll down to the Alternative Radius Server Settings section.
4. Select the Alternative Radius Server **Enabled** checkbox. The screen expands to display the Alternative Radius Server fields. The fields are identical to the fields on the Radius Server screen (see Figure 3-9 on page 46) but apply only to the selected wireless security profile.
5. Specify the fields that are explained in Table 3-7 on page 46.
6. Click **Save** or **Save to Flash & Activate** to save your settings.

Selecting the 802.1x EAPOL Version

Most wireless devices support 802.1x Extensible Authentication Protocol over LAN version 2 (EAPOL v2) for RADIUS authentication. To accommodate wireless devices that do not support EAPOL v2, you can configure the wireless access point to use both EAPOL v1 and v2.

To configure the EAPOL version:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **System** > **Security**. The Security screen displays (see Figure 3-10 on page 49).

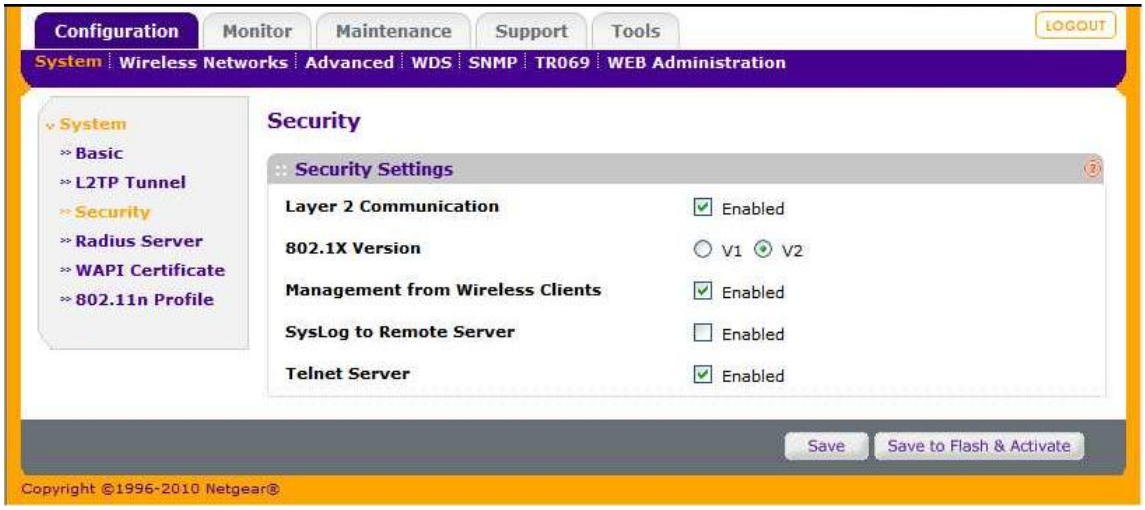


Figure 3-10

3. Next to 802.1X Version, select one of the following radio buttons:
   - **v1**. Both EAPOL v1 and v2 devices can associate with the wireless access point.
   - **v2**. Only EAPOL v2 devices can associate with the wireless access point. This is the default setting.
4. Click **Save** or **Save to Flash & Activate** to save your settings.

WAPI Certificates

You can Install WAPI certificates to be used for authentication. You will need the following information:

- Authentication Server IP - Server IP for WAPI authentication
- ASU Certification - Certificate for ASU
- User Certification - Certificate for the User Account

To install WAPI Certificates:

1. Select **Configuration** > **System** > **WAPI Certificate**. The WAPI Certificate screen displays.
2. Enter the Server address and Certificates to be uploaded.
3. Click **Install**.

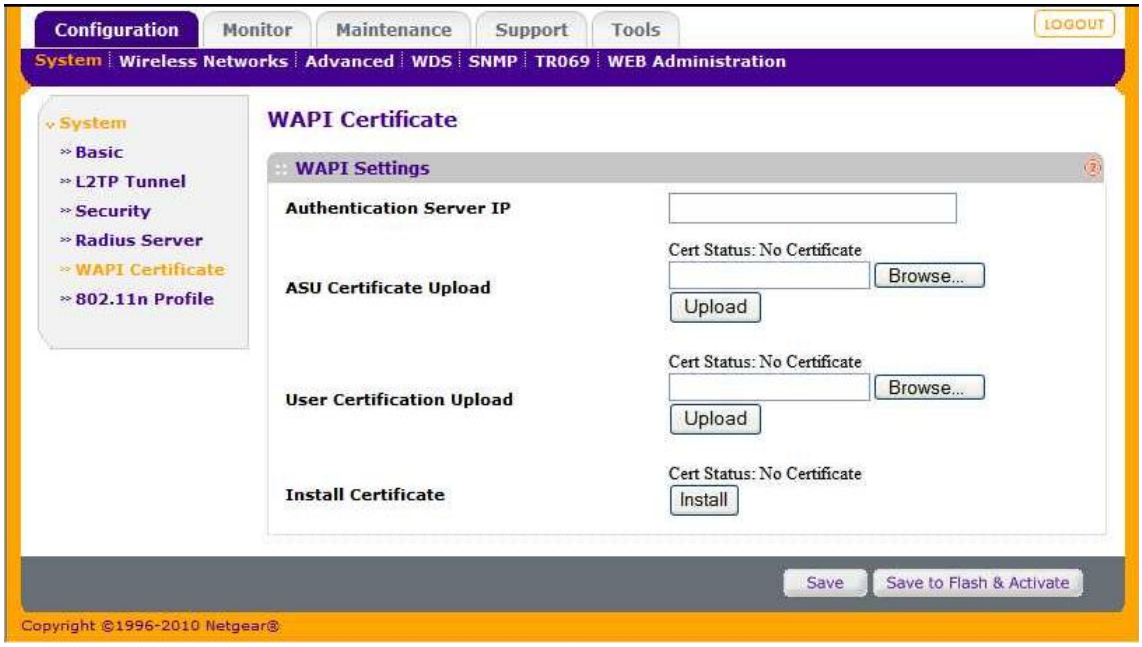


Figure 3-11

Restricting Wireless Access by MAC Address

For increased security, you can restrict access to an SSID to allow only specific computers or wireless cards based on their MAC addresses. You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the wireless access point. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

> **Note:** For wireless adapters, you can usually find the MAC address printed on the wireless adapter.

To restrict access based on MAC addresses for an individual SSID:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.

2. Select **Configuration** > **Wireless Networks**. The Wireless Networks screen opens, displaying 16 wireless security profiles (see Figure 3-2 on page 38).
3. To configure or edit a wireless security profile, select the corresponding Edit hyperlink to the right of the wireless security profile. The Edit Wireless Network screen opens for the selected wireless security profile. Scroll down to the Access Control Settings section.
4. From the Access Control pull-down menu, select one of the following options:
   - **None**. Access control is disabled. This is the default setting.
   - **Deny all except listed**. Access control is denied to all wireless clients of the SSID except for the trusted wireless clients whose MAC addresses are listed in the Listed MAC Addresses table. When you select this option, the screen expands to display the MAC Insertion Tool and the Listed MAC Addresses table, as shown in Figure 3-12 on page 51.
   - **Accept all except listed**. Access control is granted to all wireless clients of the SSID except for the wireless clients whose MAC addresses are listed in the Listed MAC Addresses table. When you select this option, the screen expands to display the MAC Insertion Tool and the Listed MAC Addresses table.

   There is one Listed MAC Addresses table to deny access and another one to grant access. Your selection from the Access Control pull-down menu determines which table is displayed (see Figure 3-12 on page 51).

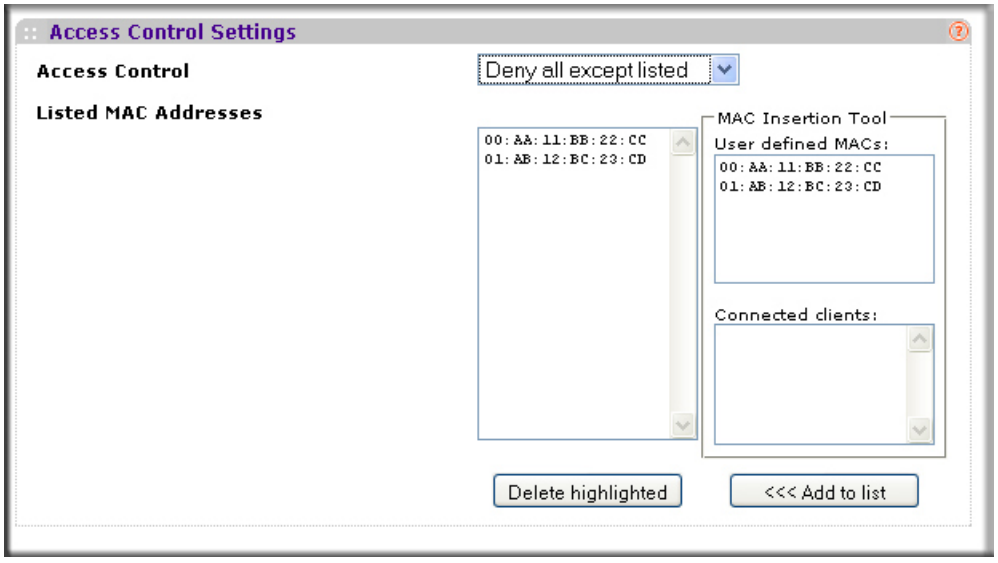


Figure 3-12

There are two methods to add MAC addresses to the Listed MAC Addresses table:

- Manually enter one or more MAC addresses in the User defined MACs window of the MAC Insertion Tool, then click **<<< Add to list**.
- Select one or more MAC addresses from the Connected clients window of the MAC Insertion Tool, then click **<<< Add to list**.

To delete MAC addresses from the Listed MAC Addresses table, select (highlight) one or more MAC addresses in the Listed MAC Addresses table, then click **Delete highlighted**.

5. Click **Save** or **Save to Flash & Activate** to save your settings.

WARNING!

When configuring the wireless access point from a wireless computer whose MAC address is not in the access control list, you will lose your wireless connection when you click Save or Save to Flash & Activate. You must then access the wireless access point from a wired computer or from a wireless computer which is on the access control list to make any further changes.

Configuring Alternate DHCP Server Settings

In addition to the general DHCP server settings for the LAN segment (see "Configuring LAN Settings" on page 23), you can specify alternate DHCP server settings for an individual SSID. DHCP requests can be relayed to a remote DHCP server or fulfilled by a local DHCP server.

To configure alternate DHCP server settings for an individual SSID:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **Wireless Networks**. The Wireless Networks screen opens, displaying 16 wireless security profiles (see Figure 3-2 on page 38).
3. To configure or edit a wireless security profile, select the corresponding Edit hyperlink to the right of the wireless security profile. The Edit Wireless Network screen opens for the selected wireless security profile. Scroll down to the DHCP Server Settings section.
4. From the DHCP Server Type pull-down menu, select one of the following options:
   - **None**. DHCP requests are forwarded to the LAN segment and not fulfilled by the wireless segment. This is the default setting.
   - **Relay**. The wireless access point forwards DHCP requests to a remote DHCP server. When you select this option, the screen expands as shown in *Figure 3-13*. Enter the IP address of the remote DHCP server in the DHCP Server IP field.

Figure 3-13

- **Server**. The wireless access point allocates and provides IP addresses locally. When you select this option, the screen expands as shown in Figure 3-14 on page 53. Specify the fields as explained in Table 3-8 on page 53. There are no default values for this screen.

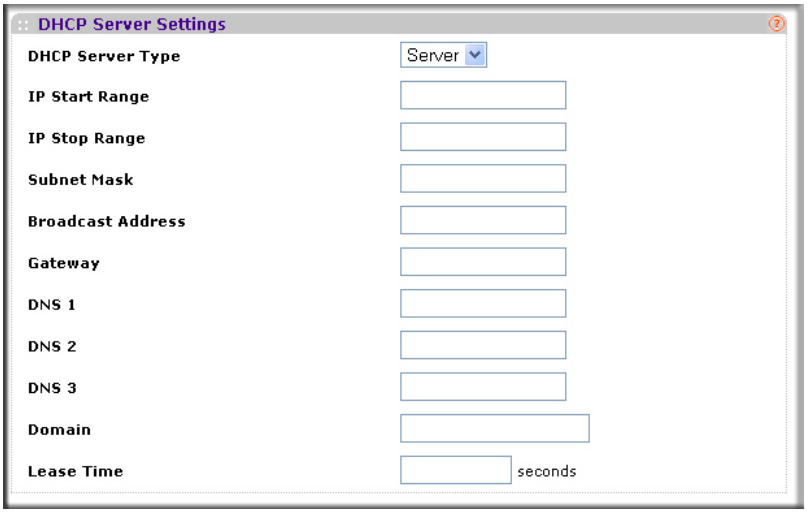


Figure 3-14

Table 3-8. Alternate DHCP Server Settings

Field	Description
IP Start Range	The first address in the range of IP addresses to be assigned to DHCP clients.
IP Stop Range	The last address in the range of IP addresses to be assigned to DHCP clients.
Subnet Mask	The subnet mask to be used by DHCP clients.
Broadcast Address	The broadcast IP address to be used by DHCP clients.
Gateway	The IP address of the default routing gateway to be used by DHCP clients.
DNS 1	The IP address of the primary static Domain Name Server (DNS) server available to DHCP clients.
DNS 2	The IP address of the secondary static DNS server available to DHCP clients.This server is used when the primary DNS server is not available.
DNS 3	The IP address of the tertiary static DNS server available to DHCP clients. This server is used when the primary and secondary DNS servers are not available.
Domain	The domain name to be used by DHCP clients.
Lease Time	The period that the DHCP server grants to the DHCP clients to use the assigned IP addresses.

5. Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring Wireless Quality of Service

To control reliability and availability of the wireless access point, you can allocate quality of service (QoS) levels per SSID. For information about general default QoS levels (Gold, Silver, and Bronze), multicast filtering, and multicast data rates, see "Configuring Basic Wireless Network Settings" on page 27, in particular *Figure 2-12* and *Table 2-7*. In addition to these general QoS settings, you can assign specific traffic bandwidth limits (also referred to as traffic shaping), filter incoming traffic, and configure advanced QoS settings, all per individual SSID.

Configuring Wireless Traffic Shaping

To set limits on the bandwidth of incoming and outgoing wireless traffic for an individual SSID:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **Wireless Networks**. The Wireless Networks screen opens, displaying 16 wireless security profiles (see Figure 3-2 on page 38).
3. To configure or edit a wireless security profile, select the corresponding Edit hyperlink to the right of the wireless security profile. The Edit Wireless Network screen opens for the selected wireless security profile. Scroll down to the Bandwidth Settings section.
4. Select the Bandwidth Management **Enabled** checkbox. The screen expands to display the Upstream Limit and Downstream Limit fields.

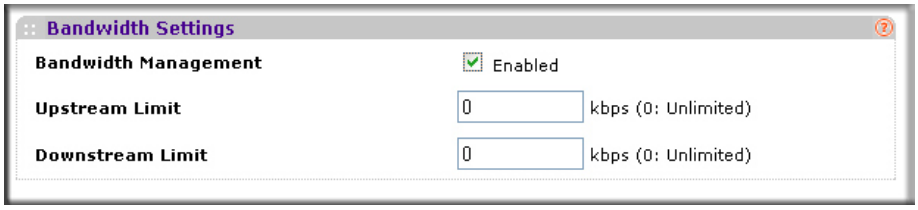


Figure 3-15

5. Specify the bandwidth limits:
   - **Upstream Limit**. Specify the bandwidth limit for outgoing traffic limit in kbps. The default is zero, which specifies unlimited bandwidth.
   - **Downstream Limit**. Specify the bandwidth limit for incoming traffic in kbps. The default is zero, which specifies unlimited bandwidth.
6. Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring Wireless Traffic Filtering

You can filter incoming wireless traffic based on MAC addresses, IP addresses, and protocols. Traffic can be either accepted or dropped.

To configure filters for incoming wireless traffic for an individual SSID:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **Wireless Networks**. The Wireless Networks screen opens, displaying 16 wireless security profiles (see Figure 3-2 on page 38).
3. To configure or edit a wireless security profile, select the corresponding Edit hyperlink to the right of the wireless security profile. The Edit Wireless Network screen opens for the selected wireless security profile. Scroll down to the Filter Settings section.
4. Select the Wireless Network Filter **Enabled** checkbox. The screen expands to display the filter fields and policy table.

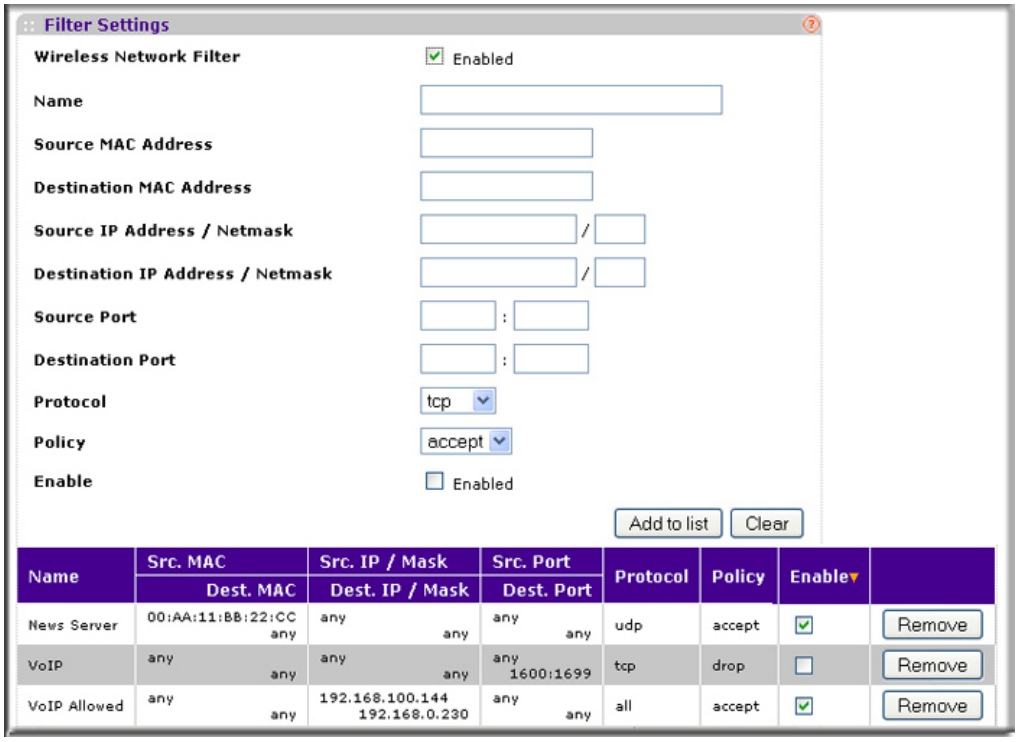


Figure 3-16

5. Specify the fields as explained in *Table 3-9*.

Table 3-9. Filter Settings

Field	Descriptions
Name	Assign a name to the filter policy.
Source MAC Address	The source MAC address of the incoming traffic
Destination MAC Address	The destination MAC address for the incoming traffic.
Source IP Address / Netmask	The source IP address and optional netmask of the incoming traffic. This field is not applicable when you select ARP as the protocol.
Destination IP Address / Netmask	The destination IP address and optional netmask for the incoming traffic. This field is not applicable when you select ARP as the protocol.
Source Port	The source port of the incoming traffic. This field is applicable only when you select TCP or UDP as the protocol.
Destination Port	The destination port for the incoming traffic. This field is applicable only when you select TCP or UDP as the protocol.
Protocol	Select the protocol(s) to which the filter rule should apply from the pull-down menu: • **tcp**. The rule applies only to incoming Transmission Control Protocol (TCP) traffic. • **udp**. The rule applies only to incoming User Datagram Protocol (UDP) traffic. • **icmp**. The rule applies only to incoming Internet Control Message Protocol (ICMP) traffic. • **arp**. The rule applies only to incoming Address Resolution Protocol (ARP) traffic. • **all.** The rule applies to incoming traffic of any protocol. This is the default setting.
Policy	Select the policy action from the pull-down menu: • **accept**. All incoming traffic that matches the policy is accepted. • **drop**. All incoming traffic that matches the policy is dropped. This is the default setting.
Enable	The policy is activated by default after you have added the policy to the policy table and you have clicked Save or Save to Flash & Activate. Deselect the **Enabled** checkbox to add the policy to the policy table without allowing it to be activated after you have clicked Save or Save to Flash & Activate.

After you have specified the filter fields, click **Add to List** to add the policy to the policy table or click **Clear** to clear the filter fields and return the settings to default.

If you want to remove a policy from the policy table, click **Remove** in the rightmost column of the policy that you want to remove.

6. Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring Advanced QoS Settings

To configure advanced QoS settings for an individual SSID:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **Wireless Networks**. The Wireless Networks screen opens, displaying 16 wireless security profiles (see Figure 3-2 on page 38).
3. To configure or edit a wireless security profile, select the corresponding Edit hyperlink to the right of the wireless security profile. The Edit Wireless Network screen opens for the selected wireless security profile. Scroll down to the Advanced Settings section.

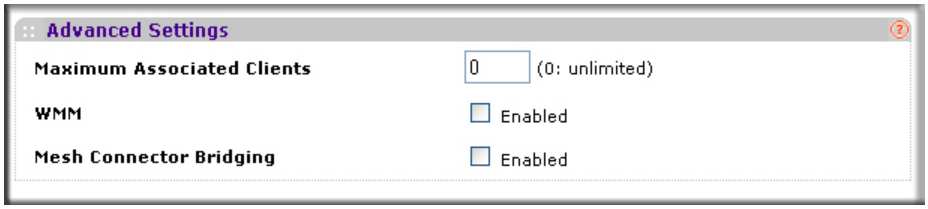


Figure 3-17

4. Specify the Advanced Settings fields as explained in *Table 3-10*.

Table 3-10. Advanced (QoS) Settings

Field	Descriptions
Maximum Associated Clients	Specify the maximum number of wireless clients that are allowed to connect to the SSID. The default setting is 0, which indicates a limitless number of wireless clients.
WMM	Wi-Fi Multimedia (WMM) is a subset of the 802.11e standard. WMM allows QoS for wireless traffic; it provides applications that require better throughput and performance special queues with higher priority. For example, time-dependent information such as video and audio are given higher priority over applications such as FTP. WMM is enabled by default for the SSID. Deselect the **Enabled** checkbox to disable WMM for the SSID. **Note**: For WMM to function correctly, wireless clients must also support WMM.
Mesh Connector Bridging	The Mesh Connector Bridging feature allows wireless devices with wireless distribution system (WDS) capability to receive packets with four addresses in the 802.11 header, thereby allowing a transparent bridge to be formed between the wireless access point and wireless devices. Mesh Connector Bridging is disabled by default for the SSID. Select the **Enabled** checkbox to enable the Mesh Connector Bridging for the SSID.

5. Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring Wireless Client Separation

Wireless client separation prevents associated wireless clients (using the same SSID) from communicating with each other, which is useful for hotspots and other public access situations. This feature is either globally enabled or globally disabled. However, per individual SSID, you can specify to allow or block unicast and/or broadcast and multicast traffic between the clients of that same SSID.

Globally Enabling Wireless Client Configuration

To enable wireless client separation:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **System** > **Security**. The Security screen displays (see Figure 3-18 on page 58).

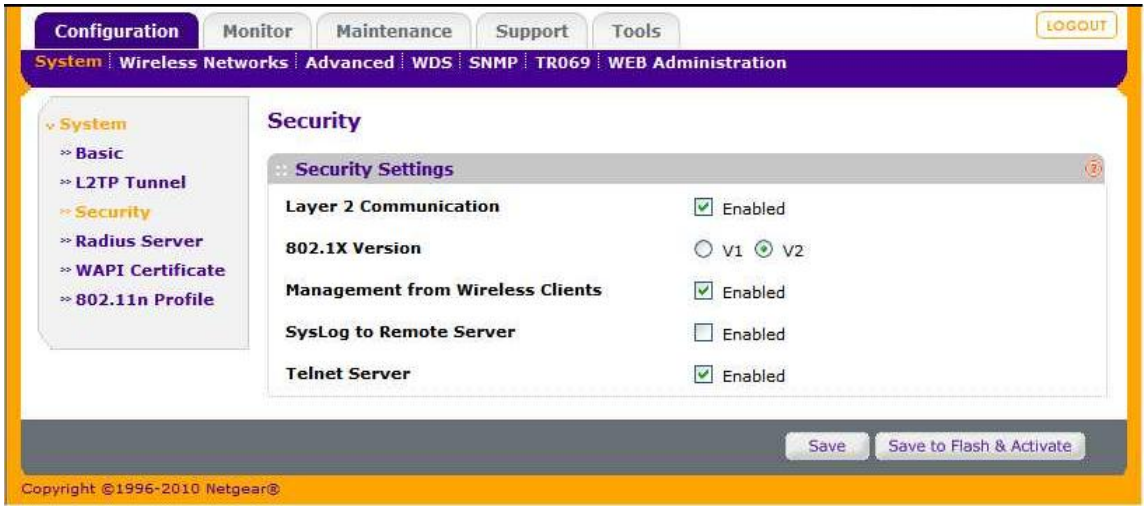


Figure 3-18

3. Next to Layer 2 Communication, select the **Enabled** checkbox. This checkbox is deselected by default.
4. Click **Save** or **Save to Flash & Activate** to save your settings.

Refining Wireless Client Separation

To configure wireless client separation for an individual SSID, and to allow or block unicast, broadcast, and multicast traffic between the clients of the same SSID:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.

2. Select **Configuration** > **Wireless Networks**. The Wireless Networks screen opens, displaying 16 wireless security profiles (see Figure 3-2 on page 38).
3. To configure or edit a wireless security profile, select the corresponding Edit hyperlink to the right of the wireless security profile. The Edit Wireless Network screen opens for the selected wireless security profile. Scroll down to the Alternative Layer 2 Communication Settings section.
4. Select the Alternative Layer 2 Communication **Enabled** checkbox. The screen expands to let you configure the wireless client separation settings.

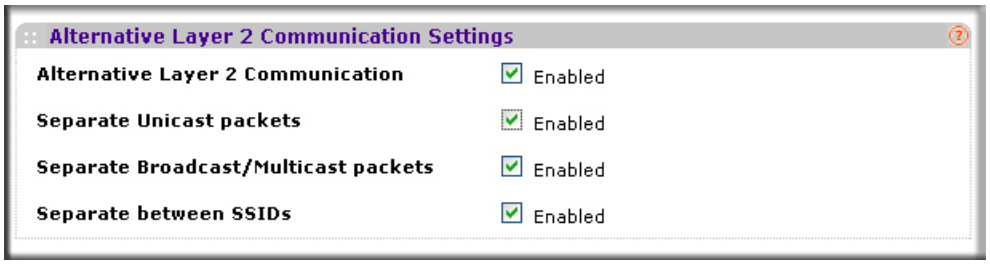


Figure 3-19

5. Enter the wireless client separation settings (also referred to as alternate Layer 2 communication settings) as explained in *Table 3-11*.

Table 3-11. Wireless Client Separation Settings

Field	Descriptions
Separate Unicast Packets	By default, unicast packets are blocked between clients of the SSID. Deselect the **Enabled** checkbox to allow unicast packets between clients of the SSID.
Separate Broadcast/Multicast packets	By default, broadcast and multicast packets are blocked between clients of the SSID. Deselect the **Enabled** checkbox to allow broadcast and multicast packets between clients of the SSID.
Separate between SSIDs	By default, communication between clients of the SSID and clients of other SSIDs is blocked. Deselect the **Enabled** checkbox to allow communication between clients of the SSID and clients of other SSIDs.

6. Click **Save** or **Save to Flash & Activate** to save your settings.

Managing Your Network

4

This chapter describes how to use the management features of your wireless access point.

This chapter includes:

- *Backing Up, Restoring, and Erasing Your Settings* ” on this page
- “Upgrading the Wireless Access Point Firmware” on page 65
- “Changing the Administrator Password and User Name” on page 66
- “Viewing Network Management Information” on page 68
- “Configuring Remote Management” on page 78
- “Scheduling Management Tasks” on page 91

Backing Up, Restoring, and Erasing Your Settings

The configuration settings of the wireless access point are stored in a configuration file in the wireless access point. From the Configuration screen, this file can be backed up to a computer, restored from a computer, or reverted to factory default settings.

To access the Configuration screen:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Maintenance** > **Config**. The Configuration screen displays (see Figure 4-1 on page 62).

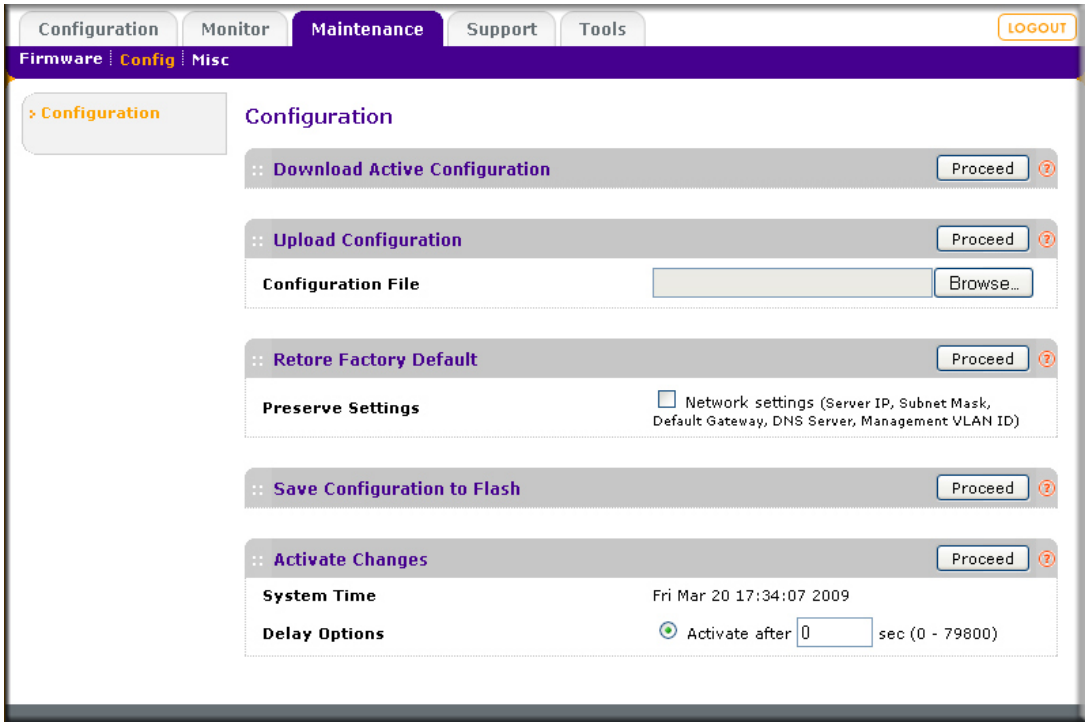


Figure 4-1

The following sections explain how to back up the configuration file, restore the configuration file, revert the configuration file to factory default settings, and perform other tasks from the Configuration screen.

Backing up the Configuration

To back up the configuration file:

1. On the Configuration screen (see *Figure 4-1*), next to Download Active Configuration, click **Proceed**.
2. Your browser extracts the configuration file from the wireless access point and prompts you for a location on your computer to store the file. You can give the file a meaningful name at this time, such as WGAP150.cfg.

Restoring the Configuration

To restore your settings from a saved configuration file:

1. On the Configuration screen (see Figure 4-1 on page 62), under Upload Configuration, enter the full path to the file in the Configuration File field, or click **Browse** to locate the file.
2. Next to Upload Configuration, click **Proceed**. If your browser requires a confirmation to proceed, confirm the action.

3. After completing the upload, the changes do not take effect until you activate them. On the Configuration screen, next to Activate Changes, click **Proceed**. If your browser requires a confirmation to proceed, confirm the action.

Rebooting and Restoring the Default Configuration

You can erase the wireless access point configurations, and return to the factory default settings. After erasing, the wireless access point's default LAN IP address will be **192.168.0.229**, the default login user name will be **admin**, and the default login password will be **password**.

Using the Software to Reboot and Restore Factory Default Settings

To use the software clear all or selected data and restore the factory default values:

1. On the Configuration screen (see Figure 4-1 on page 62), below Restore Factory Default, next to Preserve Settings, select the **Network settings** checkbox if you want to preserve the network settings such as the server IP address, subnet mask, default gateway, DNS server, and management VLAN ID. If you do not want to preserver these settings, deselect the **Network settings** checkbox.
2. Next to Restore Factory Default, click **Proceed**. If your browser requires a confirmation to proceed, confirm the action. A few seconds later, only the power LED of the wireless access point remains on, indicating that the wireless access point has rebooted.

After several minutes, the factory default configuration will be restored, and the wireless access point will be ready for use.

Using the Reset Button to Reboot and Restore Factory Default Settings

If you do not know the LAN IP address, login user name, or login password, you can still restore the factory default configuration settings with the Reset button. This button is on the rear panel of the wireless access point (see "Rear Panel" on page 11).

To use the Reset button to clear all data and restore the factory default values:

1. Push and hold the Reset button for about five seconds. (You may have to push hard.)
2. Release the Reset button. A few seconds later, only the power LED of the wireless access point remains on, indicating that the wireless access point has rebooted.

After several minutes, the factory default configuration will be restored, and the wireless access point will be ready for use.

Saving the Configuration to Flash Memory

This procedure saves any configuration changes to the internal flash memory, allowing the changes to remain active after the wireless access point has been reloaded.To save the configuration to flash memory:

On the Configuration screen (see Figure 4-1 on page 62), next to Save Configuration to Flash, click **Proceed**. If your browser requires a confirmation to proceed, confirm the action.

Scheduling to Activate the Changes

This procedure lets you schedule the activation of any configuration changes, so that changes can be activated at a time when a minimum number of users are impacted. However, this procedure does not save the changes to flash memory, so the changes are lost when you reload the wireless access point.

To schedule the activation of changes:

1. On the Configuration screen (see Figure 4-1 on page 62), in the Delay Options field below Activate Changes, enter the time in seconds that the activation should be delayed. The default is zero seconds, which means that there is no delay and the changes are activated immediately.
2. Below Activate Changes, click **Proceed**. If your browser requires a confirmation to proceed, confirm the action.

Rebooting without Restoring the Default Configuration

You can reboot the wireless access point without restoring the default configuration by using the software reboot button on the Miscellaneous screen:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Maintenance** >**Misc**. The Miscellaneous screen displays. This screen also lets you download debug information (see “Downloading Debug Information” on page 119) and displays the current firmware version.

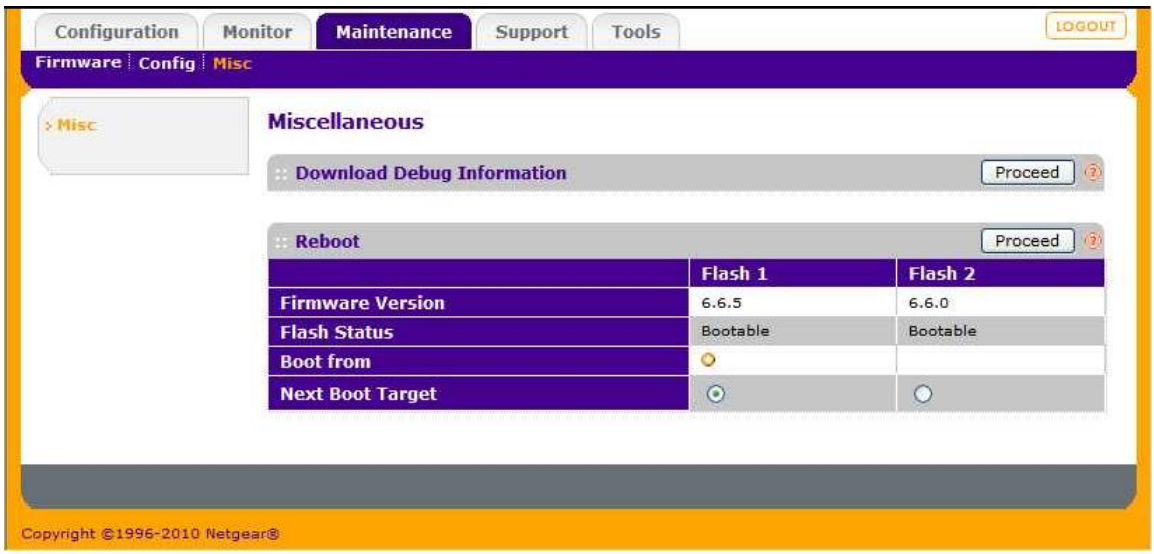


Figure 4-2

3. Next to Reboot, select the flash memory to reboot from and click **Proceed**. If your browser requires a confirmation to proceed, confirm the action. A few seconds later, only the power

LED of the wireless access point remains on, indicating that the wireless access point has rebooted.

After several minutes the wireless access point will be ready for use.

Upgrading the Wireless Access Point Firmware

WARNING!

When uploading firmware to the wireless access point, do not interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the upload may fail, corrupt the firmware, and render the wireless access point completely inoperable.

The wireless access point firmware is stored in flash memory, and can be upgraded as NETGEAR releases new firmware. You can download the upgrade file (in tar format) from the NETGEAR Web site.

Note: The Web browser used to upload new firmware into the wireless access point must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or later, or Mozilla Firefox 1.5 or later.

To upgrade the firmware on the wireless access point:

1. Download the upgrade file from NETGEAR and save it to your hard disk.
2. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
3. Back up the current configuration as described in “Backing up the Configuration” on page 62.

4. Select **Maintenance** >**Firmware**. The Firmware screen displays, showing the current firmware version. The symbol indicates the Flash module selected.

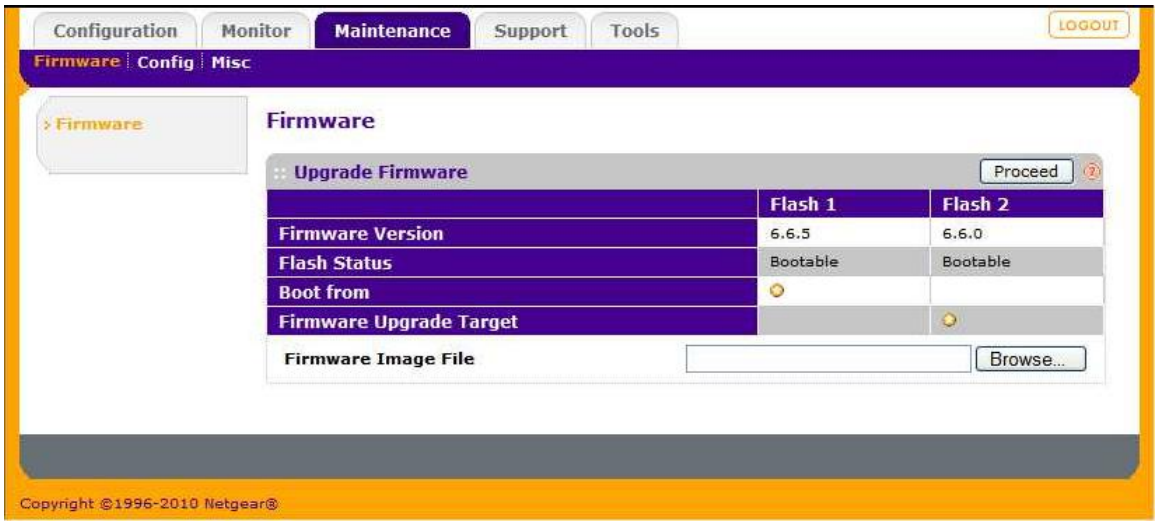


Figure 4-3

5. Next to Firmware Image File, click **Browse** to navigate to the location where the upgrade file is stored.
6. The Click **Proceed** to upgrade the firmware. If your browser requires a confirmation to proceed, confirm the action. A few seconds later, only the power LED of the wireless access point remains on, indicating that the wireless access point has rebooted.

When the upload completes, your wireless access point automatically restarts. After several minutes, the wireless access point will be ready for use. In some cases, you might need to reconfigure the wireless access point after upgrading.

Changing the Administrator Password and User Name

The default administrator user name to access the wireless access point is **admin** and the default administrator password is **password**. Change the user name to a unique name that makes sense to you and the password to a more secure password.

Tip: Be sure to change the wireless access point default password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper case and lower case), numbers, and symbols. Your password can be up to 30 characters.

Changing the Administrator Password

To change the password:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** >**WEB Administration** > **Admin Password**. The Admin Password screen displays.

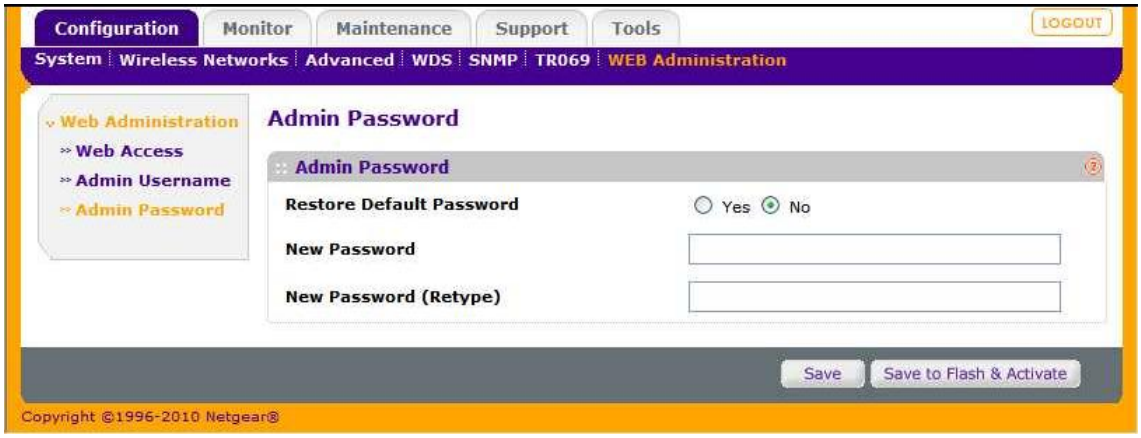


Figure 4-4

3. Next to Restore Default password, select the **No** radio button.
4. Enter the new password in the New Password field.
5. Repeat the new password in the New Password (Retype) field.
6. Click **Save** or **Save to Flash & Activate** to save your settings.

To restore the default password:

1. Next to Restore Default password, select the **Yes** radio button.
2. Click **Save** or **Save to Flash & Activate** to save your settings.

Changing the Administrator User Name

To change the user name:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.

2. Select **Configuration** >**WEB Administration** > **Admin Username**. The Admin Username screen displays.

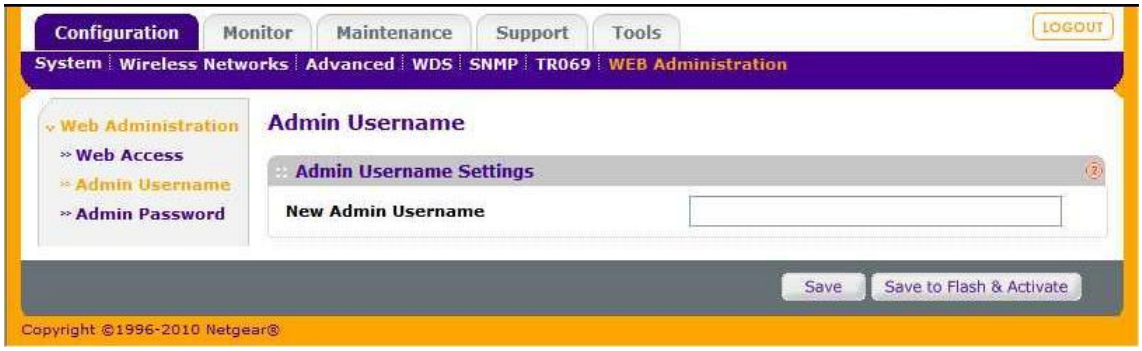


Figure 4-5

3. Enter the new user name in the New Admin Username field.
4. Click **Save** or **Save to Flash & Activate** to save your settings.

Viewing Network Management Information

The wireless access point provides a variety of status and usage information, which are discussed in the following sections.

Viewing the Activity Log

You can view the activity log on screen or send it to a syslog server.

Viewing the Activity Log on Screen

To view the activity log on screen:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.

2. Select **Monitor** > **Event Log**. The Event Log screen displays.

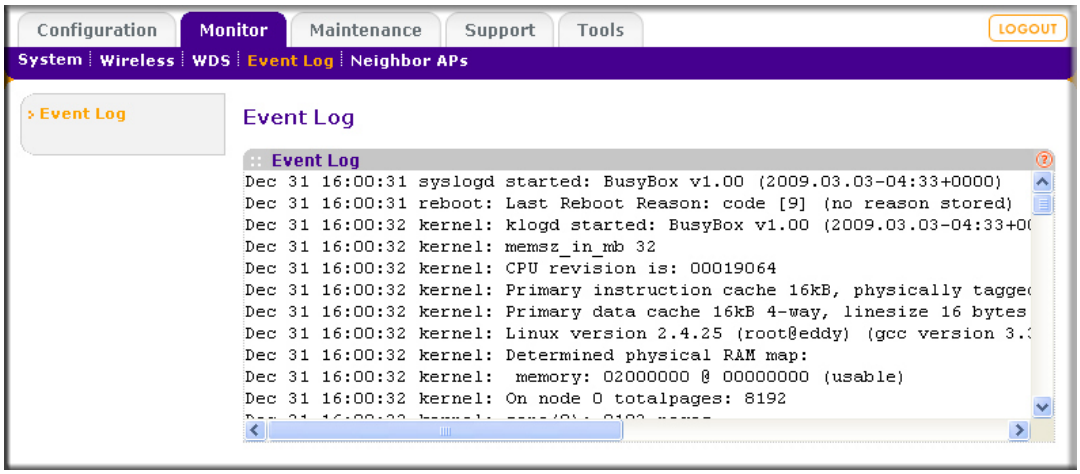

Configuration
Monitor
Maintenance
Support
Tools
LOGOUT
System | Wireless | WDS | Event Log | Neighbor APs
Event Log
Event Log
Event Log
Dec 31 16:00:31 syslogd started: BusyBox v1.00 (2009.03.03-04:33+0000)
Dec 31 16:00:31 reboot: Last Reboot Reason: code [9] (no reason stored)
Dec 31 16:00:32 kernel: klogd started: BusyBox v1.00 (2009.03.03-04:33+0
Dec 31 16:00:32 kernel: memsz_in_mb 32
Dec 31 16:00:32 kernel: CPU revision is: 00019064
Dec 31 16:00:32 kernel: Primary instruction cache 16kB, physically tagge
Dec 31 16:00:32 kernel: Primary data cache 16kB 4-way, linesize 16 bytes
Dec 31 16:00:32 kernel: Linux version 2.4.25 (root@eddy) (gcc version 3.
Dec 31 16:00:32 kernel: Determined physical RAM map:
Dec 31 16:00:32 kernel: memory: 02000000 @ 00000000 (usable)
Dec 31 16:00:32 kernel: On node 0 totalpages: 8192

Figure 4-6

The Activity Log Window displays the wireless access point's system activity.

Sending the Activity Log to a Syslog Server

To send the activity log to a syslog server:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **System** > **Security**. The Security Settings screen displays.

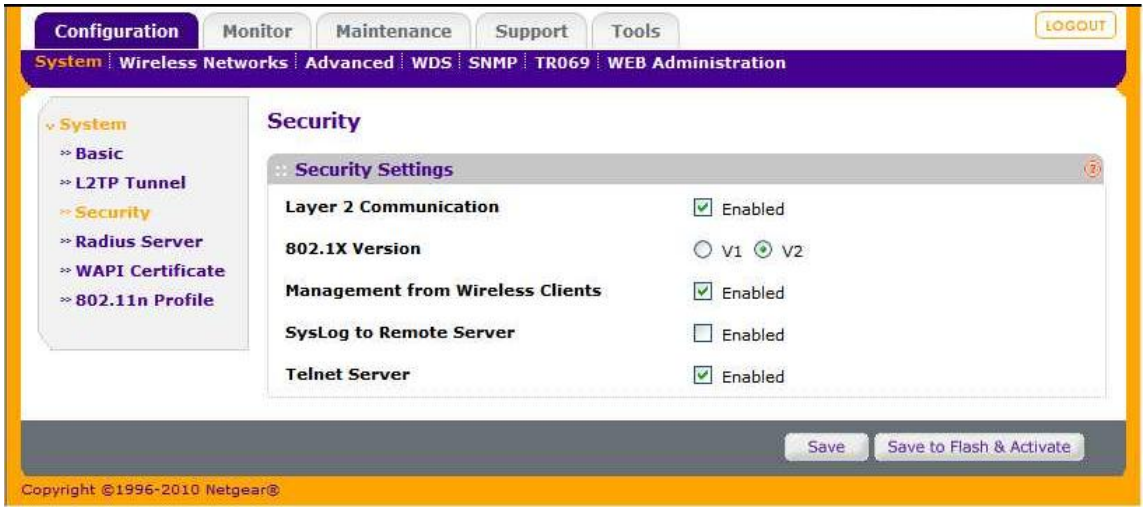


Figure 4-7

3. Select the Syslog to Remote Server **Enabled** checkbox to enable the syslog connection. The screen expands, enabling you to configure the syslog server fields.

4. Enter the syslog information in the following fields:
   - **Syslog Server Address**. The IP address of the syslog server.
   - **SysLog Server Port**. The port number for the syslog server on the LAN segment. The default port is 514.
5. Click **Save** or **Save to Flash & Activate** to save your settings.

Viewing System Information

The System Information is a summary of the wireless access point configuration settings.

To view the system information screens:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Monitor** > **System** and then **Basic**, **L2TP Tunnel**, or **Flash Management**. These three screens are shown below and their fields are explained in the tables below.

Viewing the Basic System Information Screen

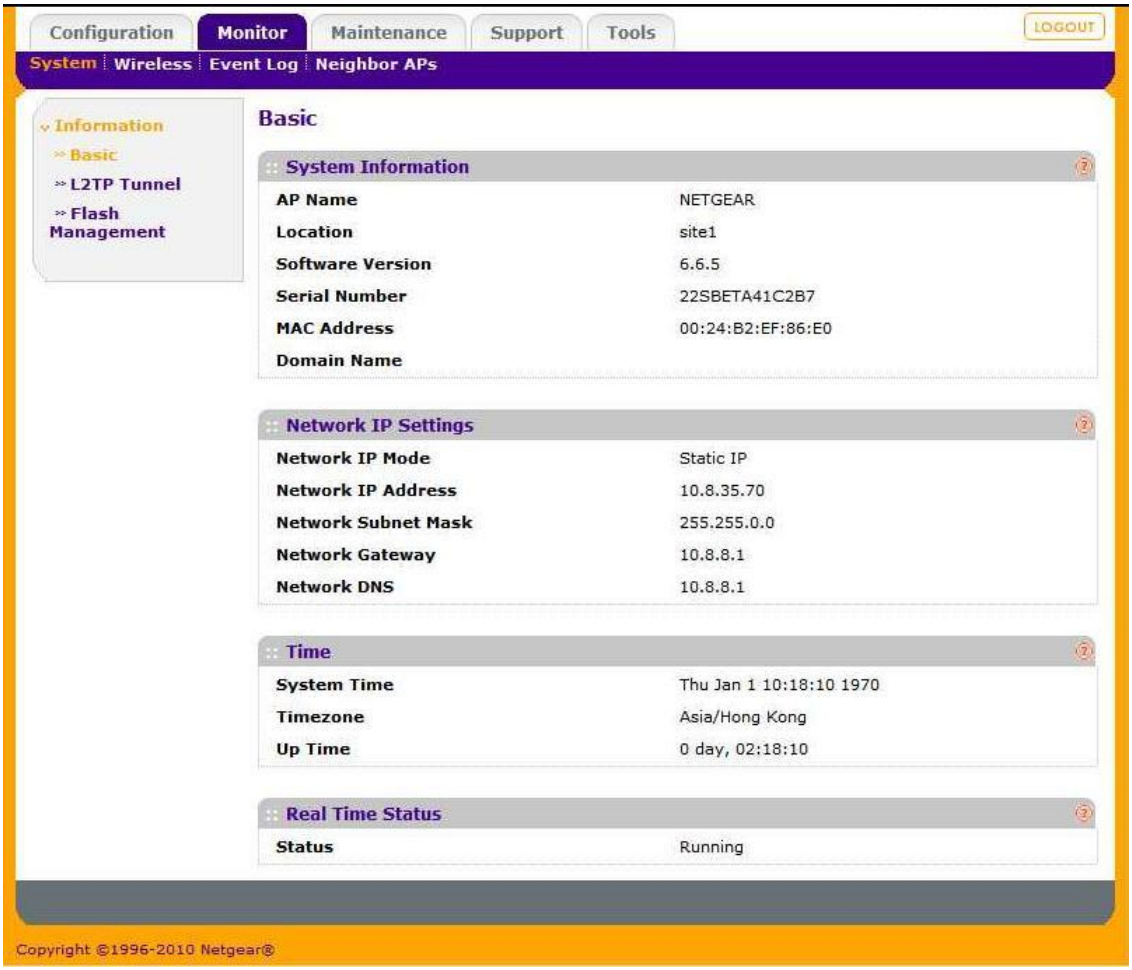


Figure 4-8

Table 4-1.

Field	Description
System Information You can configure some of these settings in "Configuring Basic System Settings" on page 19	
AP Name	The name of the wireless access point.
Location	The name of the location of the wireless access point.
Software Version	The version of the firmware currently installed.
Serial Number	The serial number of the wireless access point.
MAC Address	The MAC Address of the wireless access point's Ethernet port.

Table 4-1.

Field	Description
Domain Name	The optional name of the domain.
Network IP Settings You can configure these settings in “Configuring IP Settings” on page 20.	
Network IP Mode	The IP setting that specifies how the wireless access point acquires its IP address (DHCP, static IP, or PPPoE).
Network IP Address	The IP address of the wireless access point.
Network Subnet Mask	The subnet mask of the wireless access point.
Network Gateway	The default gateway for the wireless access point’s communication.
Network DNS	The DNS server for the wireless access point.
Time	
System Time	System time as available on the wireless access point.
Timezone	The time zone in which the wireless access point operates. To set the time zone, see “Configuring Basic System Settings” on page 19.
Up Time	The period that the wireless access point has been operating since it was turned on.
Real Time Status	
Status	The current status of the wireless access point. The modes are: • Running. The wireless access point is in operation. • Activating. The configuration is being saved and activated. • Starting up. The wireless access point is booting. • Rebooting. The wireless access point is rebooting via software.

Viewing the L2TP Tunnel Information Screen

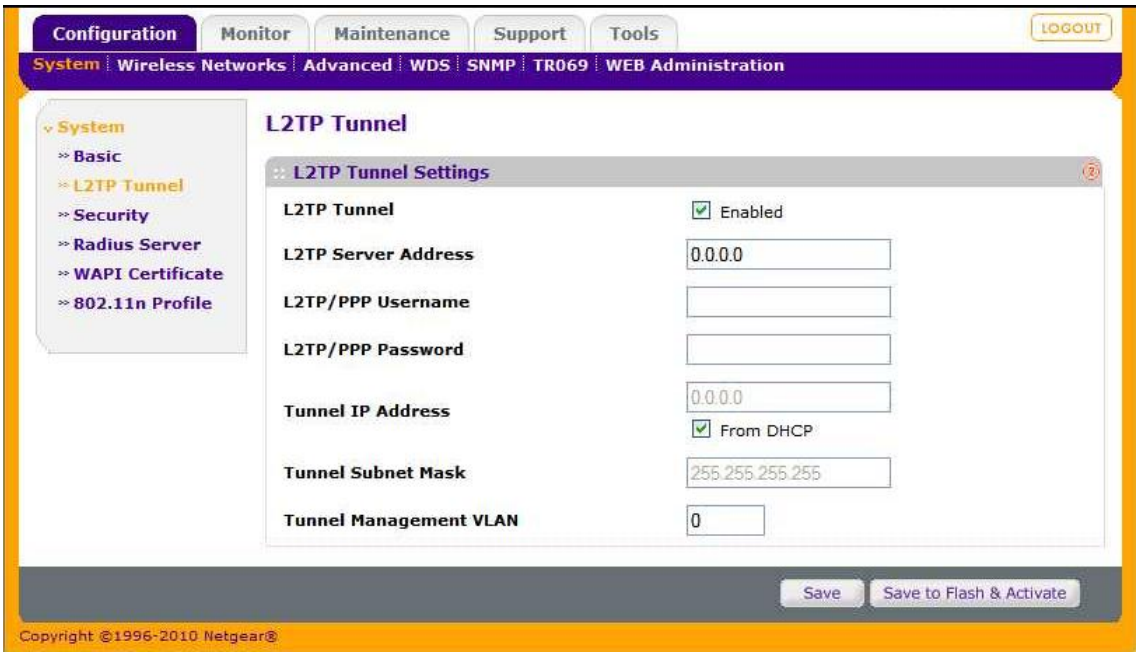


Figure 4-9

Table 4-2.

Field	Description
System Information You can configure these settings in "Configuring L2TP Tunnel Management" on page 82.	
Status	The current status of the L2TP tunnel. The modes are: • Disabled. The L2TP tunnel is torn down. • Connecting. The L2TP tunnel is in the process of being set up. • Connected. The L2TP tunnel is up.
Server Address	Address of the L2TP Server.
Username	L2TP/PPP username.
Password	L2TP/PPP password.
Tunnel IP Address	The IP address of the L2TP tunnel.
Tunnel Netmask	The subnet mask of the L2TP tunnel.
Management VLAN	Name of Management VLAN.

Viewing the Flash Management Information Screen

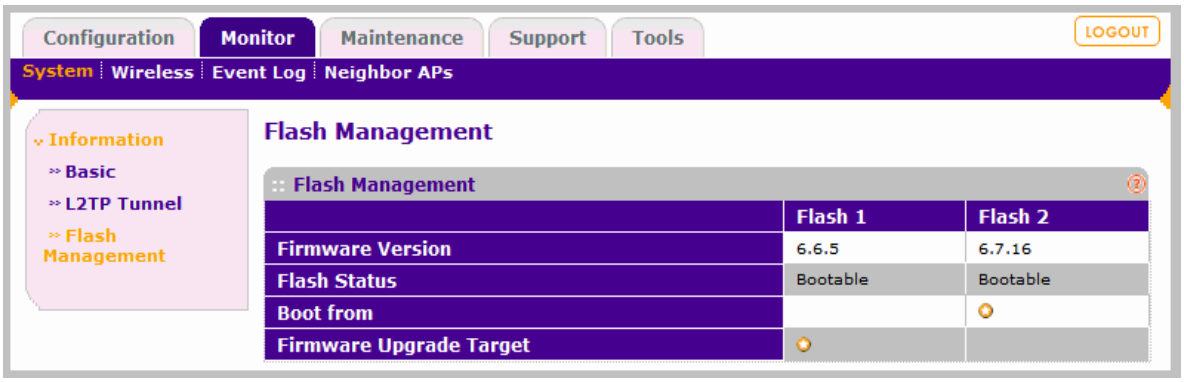


Figure 4-10

Table 4-3.

Field	Description
Flash Management	
Firmware Version	The version of the firmware currently stored in the Flash memory.
Flash Status	The status of the active flash memory. The modes are: • Bootable. The flash memory is bootable. • ---. The flash memory is not bootable.
Boot from	The indicates the Flash memory to boot from.
Firmware Upgrade Target	The indicates the Flash memory to overwrite with new firmware.

Viewing Wireless Information

To view the system information screens:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Monitor** > **Wireless** and then **Basic** or **Client**. These two screens are shown below and their fields are explained in the tables below.

Viewing the Basic Wireless Information Screen

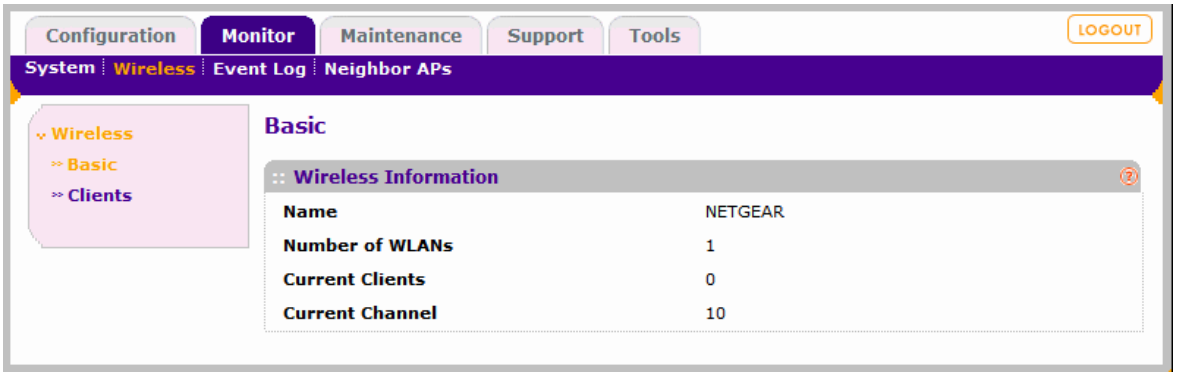


Figure 4-11

Table 4-4.

Field	Description
Wireless Information	
Name	The name of the wireless access point. To change the AP name, see "Configuring Basic System Settings" on page 19.
Number of WLANs	The number of wireless networks that are enabled on the wireless access point.
Current Clients	The number of wireless clients that are attached to the wireless access point
Current Channel	The RF channel that is in use. To change the RF channel, see "Configuring 802.11b/g Wireless Settings" on page 25.

Viewing the Wireless Clients Information Screen

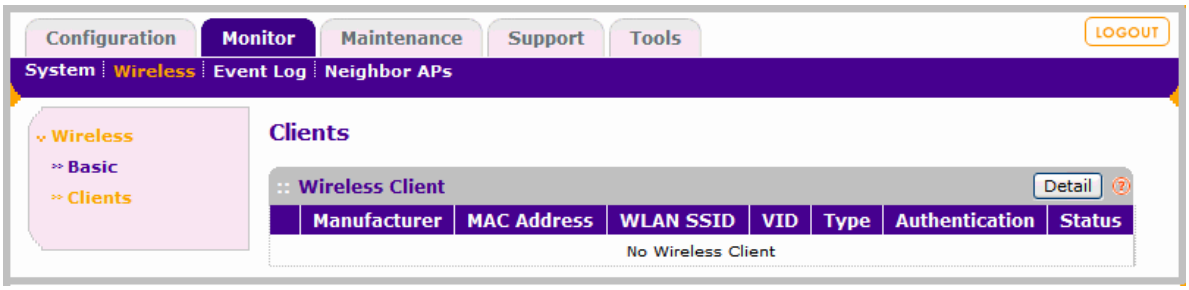


Figure 4-12

Table 4-5.

Field	Description
Wireless Client	
Manufacturer	The manufacturer of the wireless client. This information is based on the prefix of the wireless client's MAC address.
MAC Address	The wireless client's MAC address.
WLAN SSID	The wireless network to which the wireless client is attached.
VID	The VLAN ID that is used on the wireless network to which the wireless client is attached.
Type	The radio policy of the wireless client (802.11b, 802.11g, or 892.11n).
Authentication	The authentication method between the wireless client and the wireless network to which the wireless client is attached.
Status	The status of the wireless client attachment and the period that the wireless client has been attached.
Detail button	Click **Detail** to display details about each wireless client that is attached to the wireless access point.

Note: A wireless network can include multiple wireless access points, all using the same network name (SSID). This extends the reach of the wireless network. Users can roam from one wireless access point to another, providing seamless network connectivity. If this is the case, only the stations associated with this wireless access point are shown on the wireless clients information screen.

Viewing Neighbor APs Information

To view the neighbor APs information screen:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Monitor** > **Neighbor APs**. The Neighbor APs screen displays (see Figure 4-13 on page 77). Table 4-6 on page 77 explains the fields.

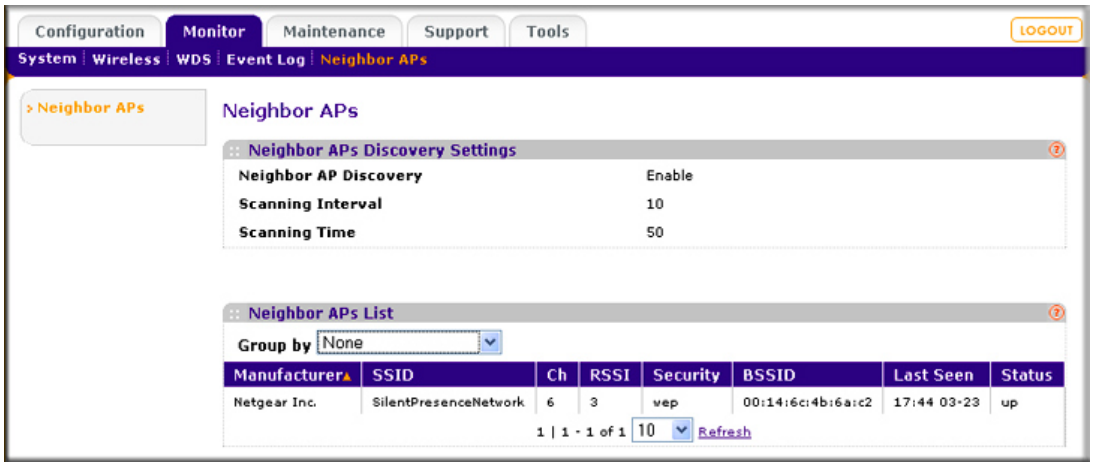


Figure 4-13

Table 4-6. Neighbor APs Information Fields

Field	Description
Neighbor APs Discovery Settings You can configure these settings in "Configuring Neighbor AP Discovery" on page 101.	
Neighbor AP Discovery	The status (enabled or disabled) of the Neighbor AP Discovery feature.
Scanning Interval	The frequency in seconds that the wireless access point scans the channels to discover neighboring APs.
Scanning Time	The time in milliseconds that the wireless access point scans a channel to discover neighboring APs.
Neighbor AP List	
Manufacturer	The manufacturer of the neighboring AP. This information is based on the prefix of the wireless client's MAC address.
SSID	The wireless network name (SSID) of the neighboring AP.
Ch	The active RF channel of the neighboring AP.
RSSI	The received signal strength indication (RSSI) of the neighboring AP.
BSSID	The MAC address of the neighboring AP.
Security	The type of wireless security of the neighboring AP.
Last Seen	The time stamp of the last scan.
Status	The state of the neighboring AP.

To sort the Neighbor APs table, use the **Group by** pull-down menu above the table or click on a column heading.

To specify the number of neighboring APs that are shown in the table, use the pull-down menu below the table and click the **Refresh** hyperlink.

Configuring Remote Management

You can remotely configure, upgrade, and check the status of your wireless access point by using a variety of methods:

- Establish an Internet connection (either wired or wireless) to the wireless access point.
- Establish an L2TP management tunnel from a server to the wireless access point
- Establish a Telnet connection.
- Use the Simple Network Management Protocol (SNMP) in a network management system.

Web Management Access

You can enable or disable the capability to log in to the wireless access point at its default LAN address of **http://192.168.0.229**, using a wired or wireless connection. This capability is enabled by default. If you disable the capability, you must use an SNMP or Telnet connection to re-enable the capability, or reset the wireless access point to its factory default settings.

Configuring Web Management Access

To configure Web management:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **WEB Administration** > **Web Access**. The Web Access screen displays (see Figure 4-14 on page 79).

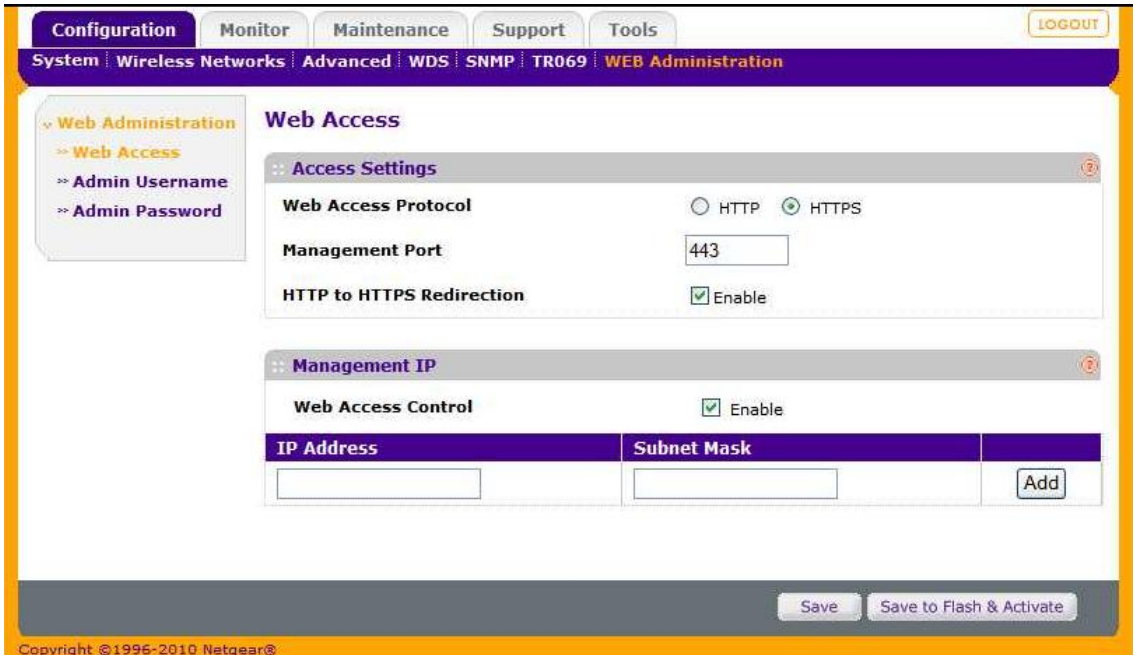


Figure 4-14

3. Complete the Web access fields and select the Web access radio buttons and checkboxes as explained in *Table 4-7*.

Table 4-7. Web Access Settings

Field	Description
Access Settings	
Web Access Protocol	Select a radio button to specify a protocol: • **HTTP**. Hypertext Transfer Protocol. • **HTTPS**. Hypertext Transfer Protocol over Secure Socket Layer. This option is more secure,
Management Port	The wireless access point's port for web management access. The default port is 80 for HTTP and 443 for HTTPS.
HTTP to HTTPS Redirection	By default, HTTP requests are automatically redirected to the HTTPS port. Deselect the **Enable** checkbox to disable this redirection.

Table 4-7. Web Access Settings (continued)

Field	Description	
Management IP		
Web Access Control	Web access control is disabled by default. Select the **Enable** checkbox to specify clients that are allowed Web management access. The screen expands to display the fields that let you add clients to the Management IP table. After you have completed these fields, click the **Add** button to add the client to the table. Only clients in the Management IP table are allowed Web management access. To delete a client from the table, click the **Del** button to the right of the client.	
	IP Address	The IP address of the client that is allowed Web management access.
	Subnet Mask	The subnet mask of the client that is allowed Web management access.

WARNING!

If you specify clients in the Management IP table but do not include the computer that you are accessing the Web management interface from, you will lose your Web management access when you click Save to Flash and Activate. You must then access the Web management interface from one of the clients that are specified in the Management IP table.

4. Click **Save** or **Save to Flash & Activate** to save your settings.

Disabling Web Management Access from Wireless Clients

As an added security measure, you can disable Web management access from wireless clients. You can still access Web management over a wired connection.

To disable Web management access from wireless clients.

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **System** > **Security**. The Security screen displays (see Figure 4-15 on page 81).

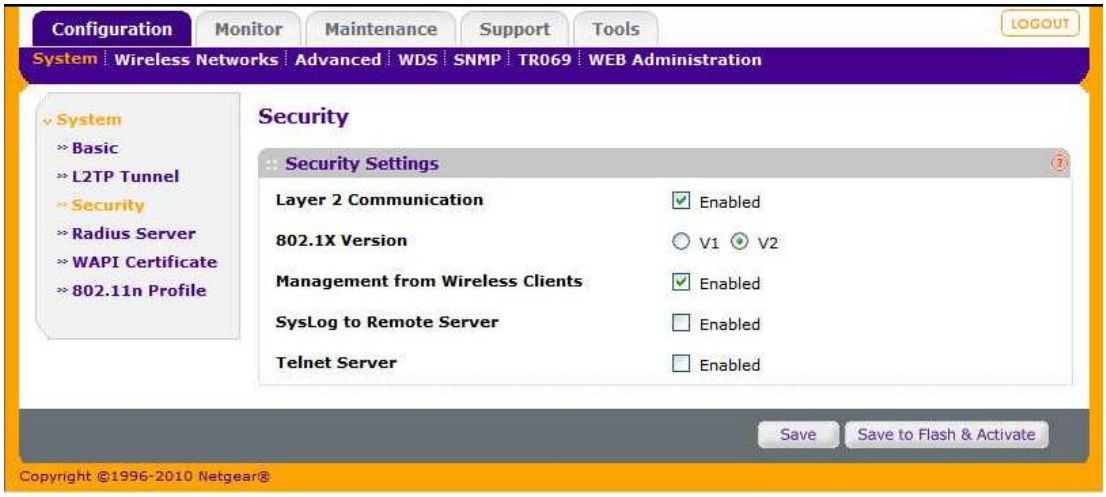


Figure 4-15

3. Next to Management from Wireless Clients, the Enabled checkbox is selected by default. To disable Web management from wireless clients, deselect the **Enabled** checkbox.

WARNING!

If you access the wireless access point from a wireless client and you disable management from wireless clients, you will lose your Web management access when you click Save to Flash and Activate. You must then access the Web management interface from a client over a wired connection.

4. Click **Save** or **Save to Flash & Activate** to save your settings

Disabling Web Management Access Entirely

Disabling Web management access entirely prevents both wired and wireless clients to log in to the wireless access point at its default LAN address of **http://192.168.0.229**.

WARNING!

If you disable Web management access entirely, you will lose your Web management access when you click Save to Flash and Activate. You must then use an SNMP or Telnet connection to re-enable Web management access, or push the Reset button to reset the wireless access point to its factory default settings.

To disable Web management:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **WEB Administration** > **Web Administration**. The Web Administration screen displays.

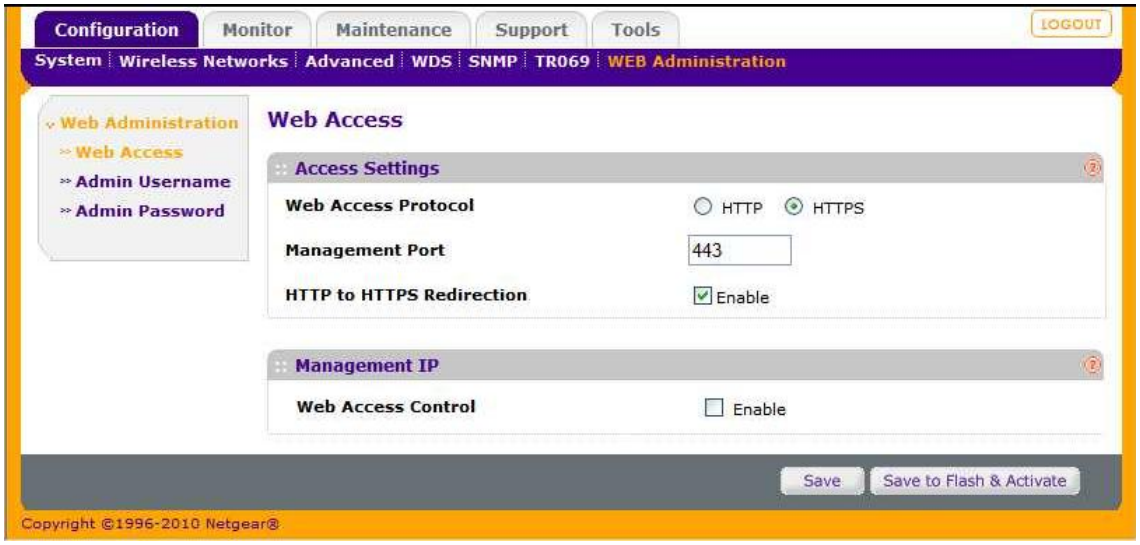


Figure 4-16

3. Next to Web Admin Interface, the Enable radio button is selected by default. To disable Web management, select the **Disable** radio button.
4. Click **Save** or **Save to Flash & Activate** to save your settings

Configuring L2TP Tunnel Management

An L2TP tunnel from the wireless access point to a server allows for centralized traffic management.

To configure L2TP tunnel management:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **System** > **L2TP Tunnel**.
3. Select the L2TP Tunnel **Enabled** checkbox. The screen expands to let you configure the L2TP tunnel settings (see Figure 4-17 on page 83).

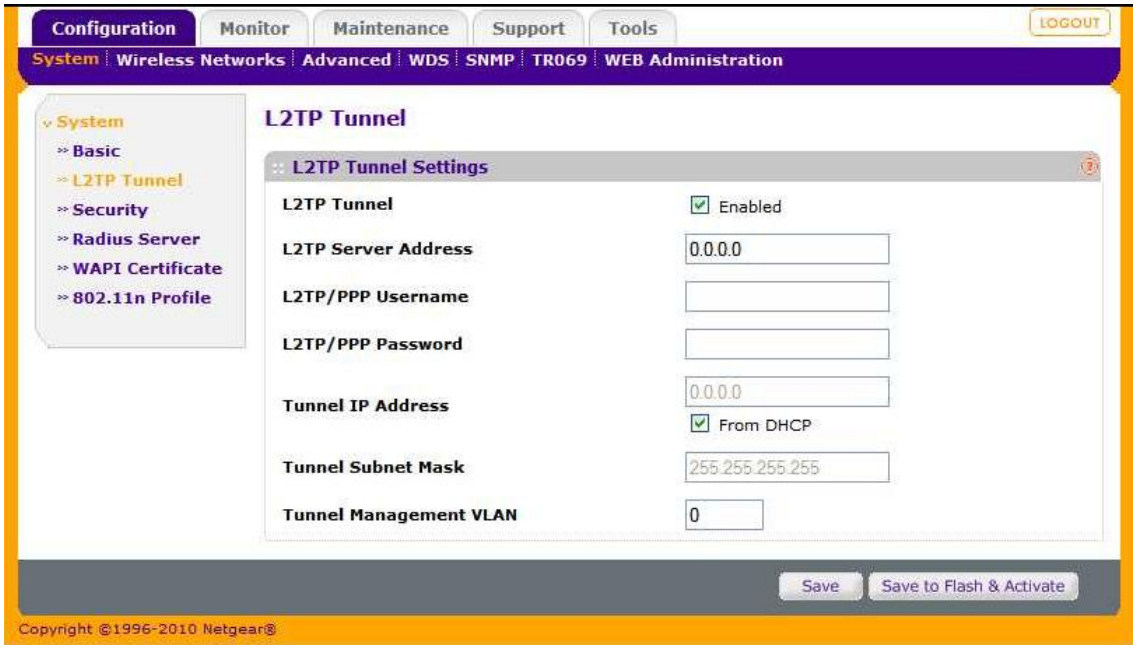


Figure 4-17

4. Complete the L2TP tunnel fields and select the L2TP tunnel checkboxes as explained in *Table 4-8*. These settings are typically provided by your Internet Service Provider (ISP).

Table 4-8. L2TP Tunnel Settings

Field	Description
L2TP Server Address	Enter the IP address of the server with which the wireless access point establishes an L2TP tunnel.
L2TP/PPP Username	Enter the user name to access the L2TP server.
L2TP/PPP Password	Enter the password to authenticate your connection with the L2TP server.
From DHCP	By default, the IP address and subnet mask for the wireless access point are acquired from a DHCP server over the L2TP tunnel. Deselect the **From DHCP** checkbox to enter the tunnel IP address and tunnel subnet mask in the following fields.
Tunnel IP Address	Enter the wireless access point's IP address to communicate with the L2TP server over the L2TP tunnel. **Note**: This field is applicable only if the From DHCP checkbox is deselected.
Tunnel Subnet Mask	Enter the wireless access point's subnet mask to communicate with the L2TP server over the L2TP tunnel. **Note**: This field is applicable only if the From DHCP checkbox is deselected.
Tunnel Management VLAN	Specify the VLAN ID from which Web management access is allowed over the L2TP tunnel. The default settings is zero, which means that Web management access is allowed from any VLAN.

5. Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring Telnet Server Access

You can allow a remote host to establish a Telnet connection to the wireless access point over the LAN port. The following Telnet commands are supported on the wireless access point:

```
Set SSID (sets the SSID)
Set Channel (sets the channel)
Set Radio Mode (sets the radio mode to b, b/g, or g-only)
Set Data Rate (sets the data rate to auto or fixed)
Get Firmware Version (shows the firmware version)
Get Serial Number (shows the serial number)
Get Lan MAC Address (shows the LAN MAC address)
Get Wi-Fi MAC Address (shows the wireless interface MAC address)
Apply Config (Restart Connection) (re-applies the configuration)
Clear Config (clears the configuration)
Reboot (reboots the unit)
```

To allow Telnet access from a remote host:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **System** > **Security**. The Security screen displays (see Figure 4-18 on page 85).

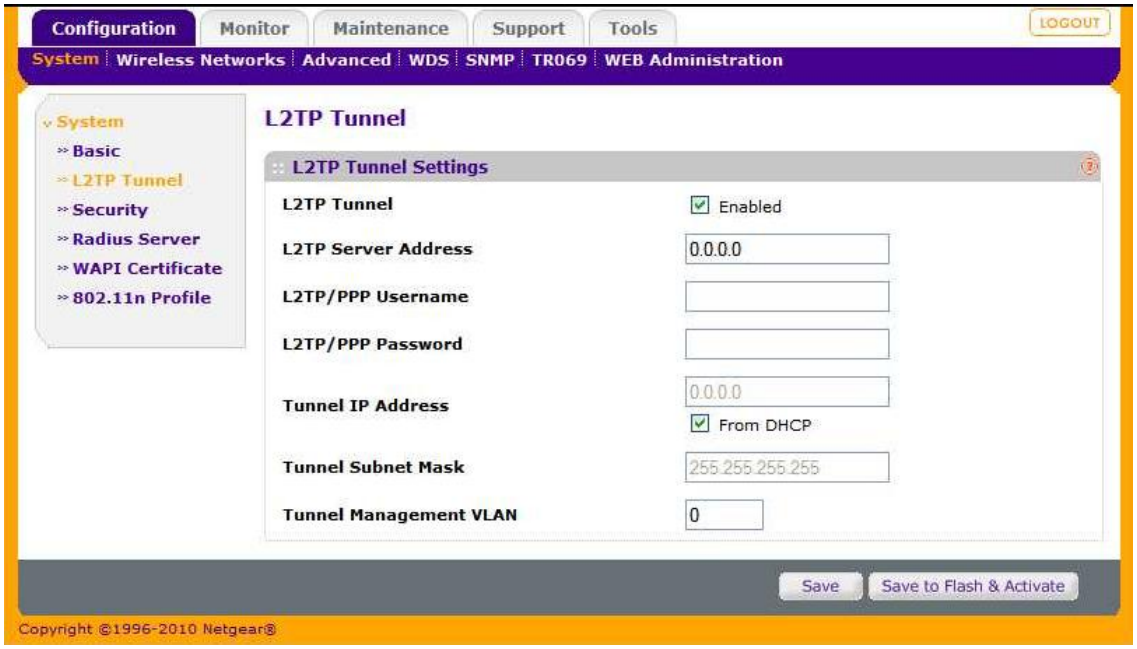


Figure 4-18

3. Next to Telnet Server, select the **Enabled** checkbox. This checkbox is deselected by default.
4. Click **Save** or **Save to Flash & Activate** to save your settings.

SNMP Remote Management

SNMP forms part of the internet protocol suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications

Enable SNMP to allow SNMP network management software such as HP OpenView to manage the wireless access point via the SNMPv1, SNMPv2, and/or SNMPv3 protocol.

Configuring SNMP Settings

To configure and enable SNMP:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **SNMP** > **Basic**. The SNMP Basic Settings screen displays (see Figure 4-19 on page 86).

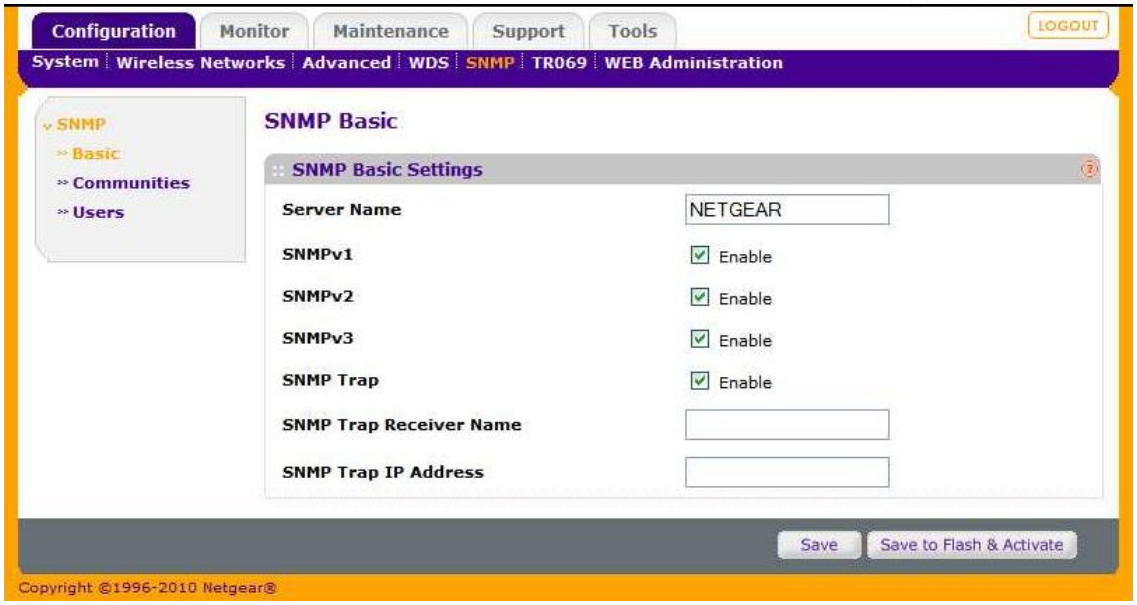


Figure 4-19

3. Complete the basic SNMP fields and select the basic SNMP checkboxes as explained in *Table 4-9*.

Table 4-9. SNMP Basic Settings

Field	Description
Server Name	Assign a unique name to the SNMP server. The default name is NETGEAR.
SNMPv1	SNMP version 1 (SNMPv1) is supported by default. Deselect the **Enable** checkbox to disable support for SNMPv1.
SNMPv2	SNMP version 2 (SNMPv2) is supported by default. Deselect the **Enable** checkbox to disable support for SNMPv2.
SNMPv3	SNMP version 3 (SNMPv3) is supported by default. Deselect the **Enable** checkbox to disable support for SNMPv3.
SNMP Trap	SNMP traps are enabled by default. Deselect the **Enable** checkbox to disable SNMP traps.
SNMP Trap Receiver Name	Enter the name of the device that should receive the traps that are sent from the wireless access point.
SNMP Trap IP Address	Enter the IP address of the device that should receive the traps that are sent from the wireless access point.

4. Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring SNMP Communities

To configure SNMP communities:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **SNMP** > **Communities**. The SNMP Communities Settings screen displays.

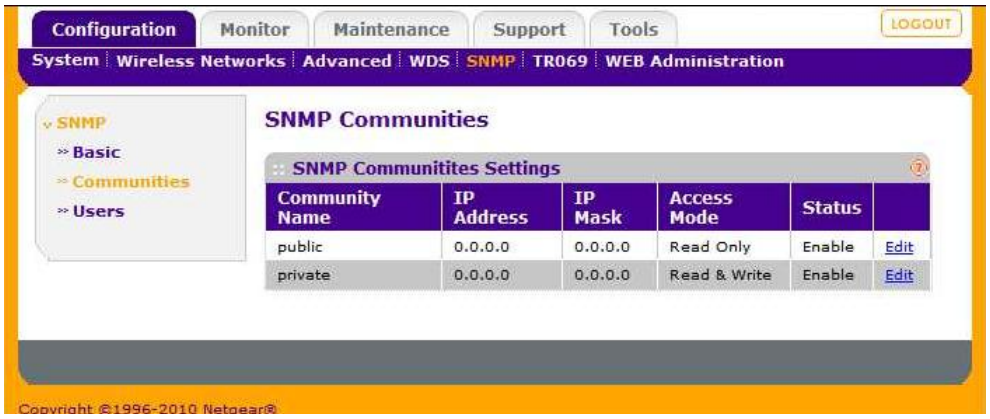


Figure 4-20

3. Click the **Edit** hyperlink for one of the two communities in the SNMP Communities Settings table. The Edit Communities screen displays.

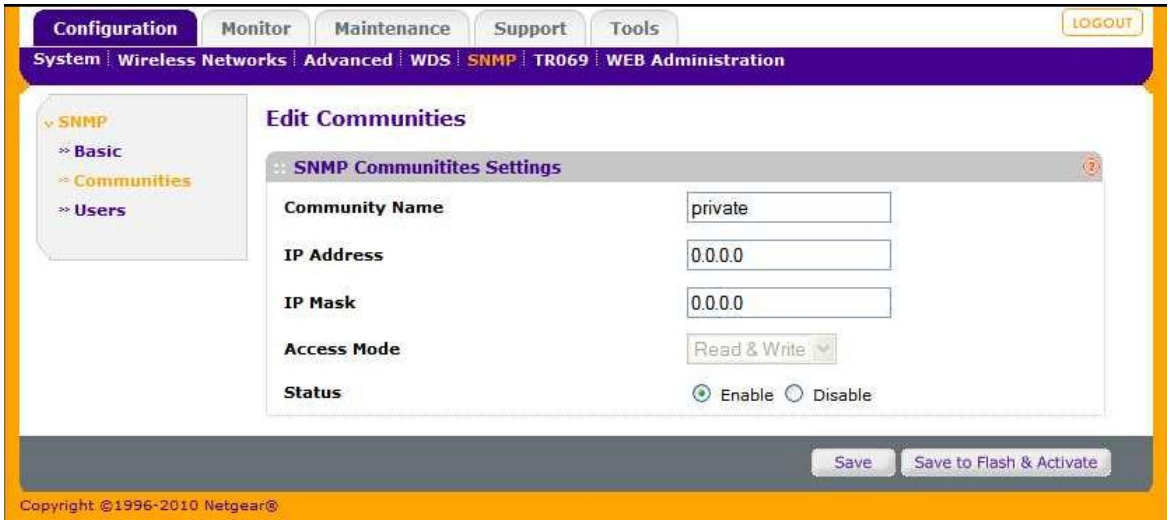


Figure 4-21

4. Complete the SNMP community fields and select the Status checkbox as explained in *Table 4-10*.

Table 4-10. SNMP Community Settings

Field	Description
Community Name	The community string to allow the SNMP manager to access the MIB objects of the wireless access point. The default setting is public (for Access Mode “Read Only”) or private (for Access Mode “Read & Write”).
IP Address	The IP address of the SNMP manager that is allowed to access the MIB objects of the wireless access point.
IP Mask	The subnet masks of the SNMP manager that is allowed to access the MIB objects of the wireless access point.
Access Mode	This field cannot be changed: the setting is “Read Only” for the SNMP community with the default name “public” and “Read & Write” for the SNMP community with the default name “private.”
Status	Select the **Enable** radio button to allow the community to access the MIB objects of the wireless access point. If you want to configure but not enable the community, select the **Disable** radio button.

5. Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring SNMP Users

SNMPv3 allows users that are allowed to access an SNMP agent to be authenticated and communication with the SNMP agent to be encrypted.

To configure individual SNMPv3 users and security:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **SNMP** > **Users**. The SNMP Users Settings screen displays (see Figure 4-22 on page 89).

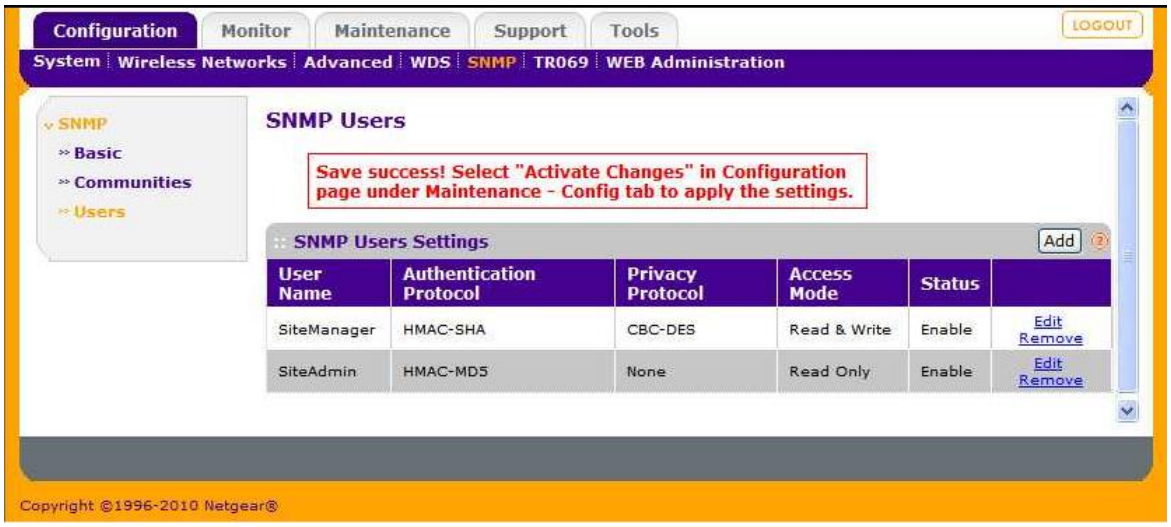


Figure 4-22

3. Take one of the following actions:

- Click the **Add** button to add a new SNMP user. The Edit Users screen displays (see Figure 4-23 on page 89).
- Click the **Edit** hyperlink to the right of an existing user in the SNMP Users Settings table. The Edit Users screen displays (see Figure 4-23 on page 89).
- Click the **Remove** hyperlink to the right of an existing user in the SNMP Users Settings table to delete the user.

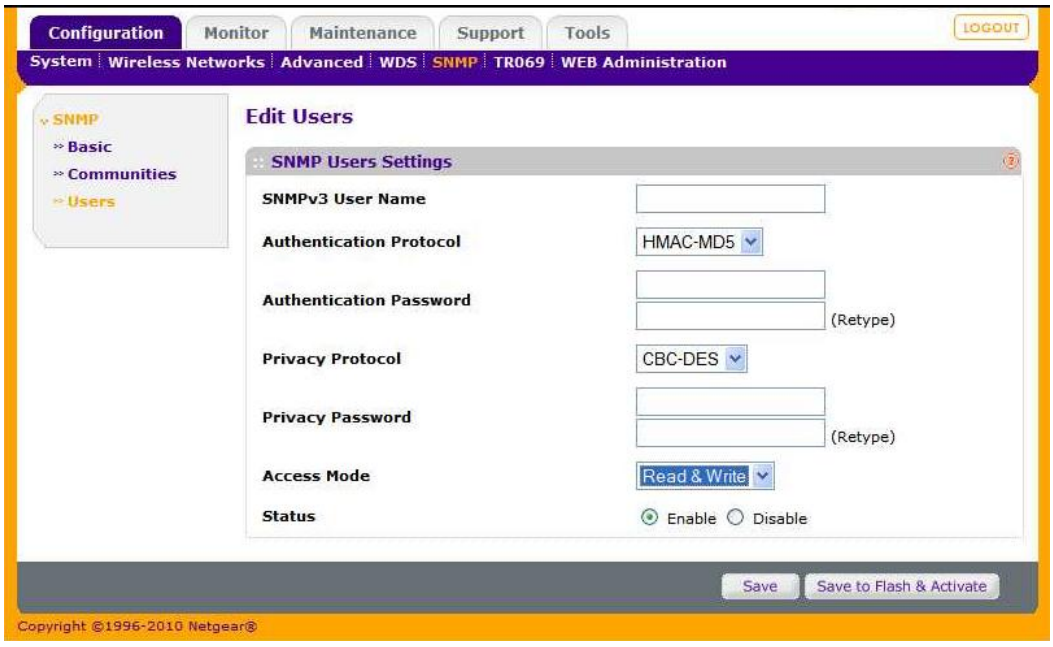


Figure 4-23

4. If you selected to add or edit an SNMP user, complete the SNMP user fields and select a Status checkbox as explained in *Table 4-11*.

Table 4-11. SNMP User Settings

Field	Description
SNMPv3 User Name	The name of the SNMPv3 user that is allowed to access the SNMP agent that collects the MIB objects from the wireless access point.
Authentication Protocol	The protocol for authenticating the SNMPv3 user. This pull-down menu lets you select one of the following authentication protocols: • **HMAC-MD5**. Hashing for Message Authentication (HMAC) algorithm in combination with Message Digest 5 (MD5). • **HMAC-SHA**. HMAC in combination with Secure Hash Algorithm (SHA).
Authentication Password	The password that an SNMPv3 user must enter to be granted access to the SNMP agent that collects the MIB objects from the wireless access point.
Privacy Protocol	The encryption method for the communication between the SNMPv3 user and the SNMP agent that collects the MIB objects from the wireless access point. This pull-down menu lets you select one of the following options: • **None**. No encryption method. • **CBC-DES**. Cipher Block Chaining (CBC) mode to the Data Encryption Standard (DES) algorithm.
Privacy Password	The password that an SNMPv3 user must enter to allow decryption of the MIB objects that the SNMP agent collects from the wireless access point. This field is applicable only when you select CBC-DES as the privacy protocol.
Status	Select the **Enable** checkbox to allow the SNMPv3 user to access the SNMP agent that collects the MIB objects of the wireless access point. If you want to configure but not enable the SNMPv3 user, select the **Disable** checkbox.

5. Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring TR069 Operation

TR-069 feature provides secure communication between the CPE and an Auto-Configuration Server (ACS). The CPE WAN Management Protocol defines the mechanism to control CPE configuration, CPE firmware and other management functions into a common framework.

The following settings and options are available: Enabled, ACS Server URL, ACS Username, ACS Password, Periodic Inform Interval

Enable/Disable - TR069 client

ACS Server URL - Defines ACS server specific URL

ACS Username - Defines ACS Username for TR069 login

ACS Password - Defines ACS password for TR069 login

Periodic Inform Interval - Interval for client to push information to ACS server

To configure TR-069 operation:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **TR069**. The TR-069 Settings screen displays.

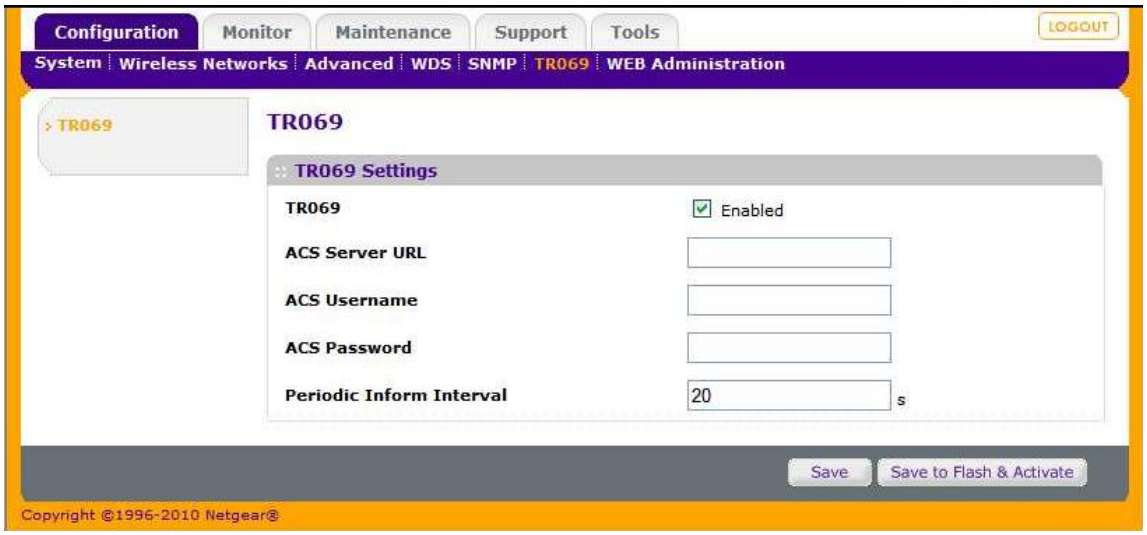


Figure 4-24

3. Enter the Server address, user name, password, and interval to be used for TR-069 management.
4. Click **Save** (or **Save & Activate**).

Scheduling Management Tasks

You can schedule management tasks to be performed at a time that you expect that there will be minimal network traffic. These tasks include automatically rebooting the wireless access point and automatically letting the wireless access point select the best RF channels to avoid a congested channels. The best RF channel selection will occur only if there are no clients associated with the wireless access point at the time that the automatic channel selection is scheduled.

To schedule management tasks:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.

2. Select **Configuration** > **Advanced** > **Schedule**. The Schedule Tasks screen displays.

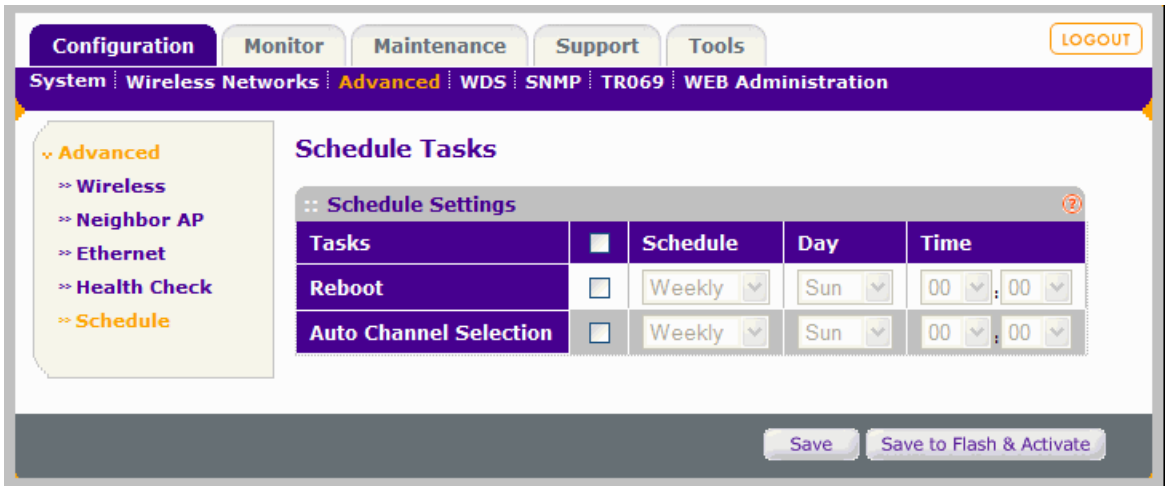


Figure 4-25

3. Schedule one or both tasks for the wireless access point as explained in *Table 4-12*.

Table 4-12. Schedule Tasks Settings

Task	Field	Description
Reboot	Checkbox	Select the checkbox next to Reboot to enable a previously scheduled reboot task or to configure a reboot task. **Note**: To enable and/or configure all tasks, select the checkbox next to Tasks in the table heading.
	Schedule	Select Monthly, Weekly, or Daily.
	Day	If monthly, select the day of the month; if weekly, select the day of the week.
	Time	Select the hour and minutes.
Auto Channel Selection	Checkbox	Select the checkbox next to Auto Channel Selection to enable a previously scheduled channel selection task or to configure a channel selection task. **Note**: To enable and/or configure all tasks, select the checkbox next to Tasks in the table heading.
	Schedule	Select Monthly, Weekly, or Daily.
	Day	If monthly, select the day of the month; if weekly, select the day of the week.
	Time	Select the hour and minutes.

4. Click **Save** or **Save to Flash & Activate** to save your settings.

Accessing Online Documentation

This reference manual (also referred to as user manual) is accessible from the Web interface.

To access the reference manual online from the Web interface:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Support**.
3. Click on the user manual hyperlink for the wireless access point.

Advanced Configuration

5

This chapter describes how to configure the advanced features of your wireless access point. This chapter includes:

- *Configuring Ethernet Links* on this page.
- "Configuring Hotspots (Captive Portals)" on page 96
- "Configuring Advanced Wireless Settings" on page 98
- "Configuring Neighbor AP Discovery" on page 101
- "Configuring Wireless Bridging and Repeating" on page 102

Configuring Ethernet Links

The Ethernet link settings allow you to select the type of Ethernet link for the wireless access point.

To configure Ethernet links:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **Advanced** > **Ethernet**. The Ethernet settings screen displays.

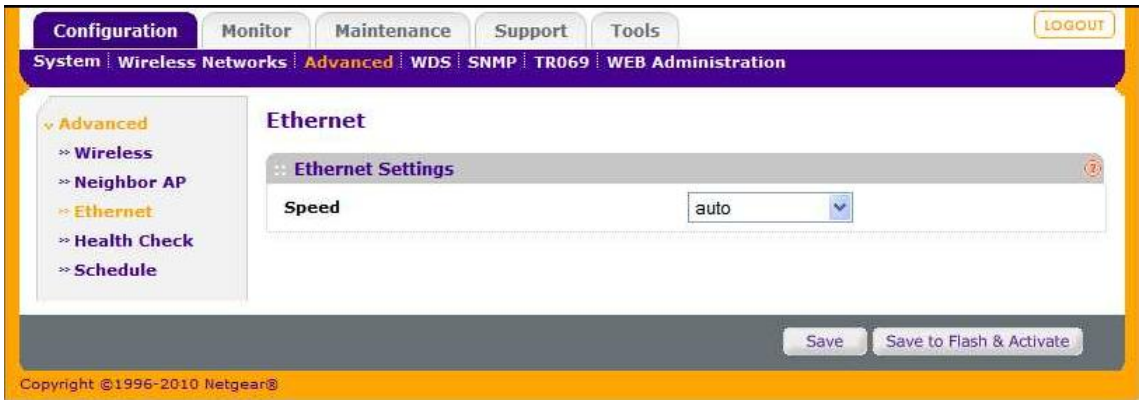


Figure 5-1

3. From the **Speed** pull-down menu, select one of the following options:
   - **auto**. Detects and sets the speed and type of the Ethernet link automatically.
   - **100baseTx-FD**. 100-Mbps full-duplex speed.
   - **100baseTx-HD**. 100-Mbps half-duplex speed.
   - **10baseT-FD**. 10-Mbps full-duplex speed.
   - **10baseT-HD**. 10-Mbps half-duplex speed.
   - **Manual**. Lets you select from four different speeds and types:
   - Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring Hotspots (Captive Portals)

If you want the wireless access point to capture and redirect the first HTTP or HTTPS request, use the Hotspot feature (also referred to as the Captive Portal feature). For example, a hotel might want to direct all wireless connections to its server to start a billing transaction, or an ISP might want to direct wireless connections to a login page.

To configure hotspots:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **Wireless Networks**. The Wireless Networks screen opens, displaying 16 wireless security profiles (see Figure 3-2 on page 3-38).
3. To configure hotspots for a wireless security profile, select the corresponding Edit hyperlink to the right of the wireless security profile. The Edit Wireless Network screen opens for the selected wireless security profile. Scroll down to the Portal Settings section.
4. Select the Captive Portal **Enable** checkbox. The screen expands to let you configure the hotspot settings (see Figure 5-2 on page 5-97).

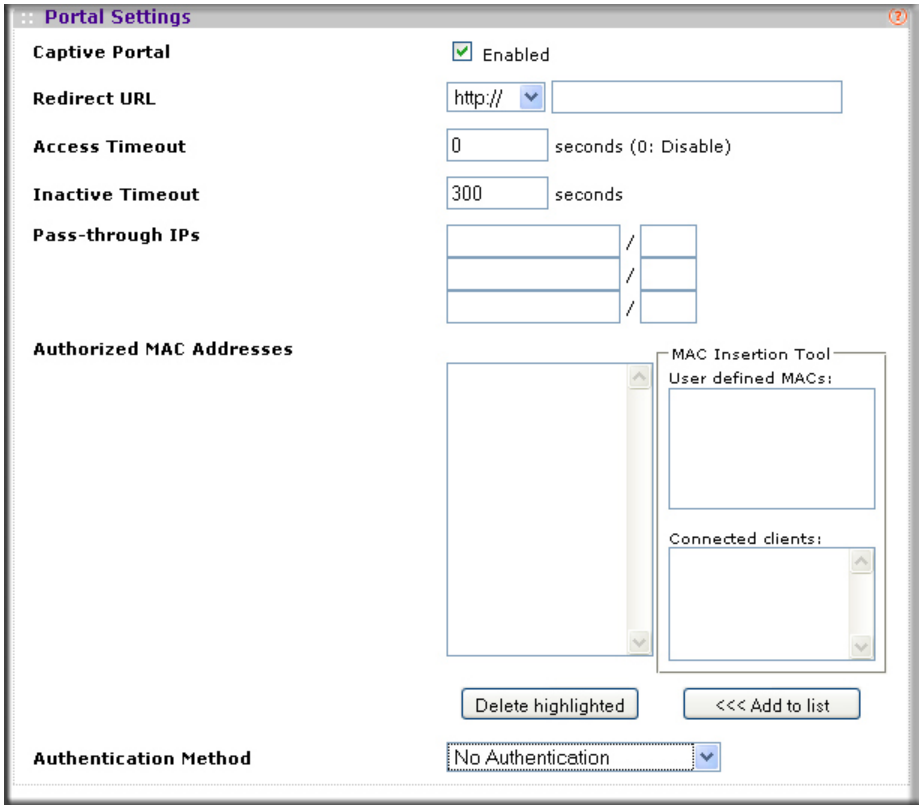


Figure 5-2

5. Enter the hotspot settings as explained in *Table 5-1*.

Table 5-1. Hotspot (or Captive Portal) Settings

Field	Description
Redirect URL	Select one of the following options from the pull-down menu: • **HTTP**. The URL to which the user must be redirected starts with HTTP. • **HTTPS**. The URL to which the user must be redirected starts with HTTPS. To the right of the pull-down menu, enter the URL to which the user must be redirected.
Authentication URL	Select one of the following options from the pull-down menu: • **HTTP**. The URL for user authentication starts with HTTP. • **HTTPS**. The URL for user authentication starts with HTTPS. To the right of the pull-down menu, enter the URL for user authentication.
Access Timeout	The time in seconds after which the user is redirected to the Redirect URL. The default is zero, which means that redirection is disabled and the user is not automatically redirected to the Redirect URL.
Inactive Timeout	The time in seconds after which the user must be re-authenticated. The default is 300 seconds (5 minutes).

Table 5-1. Hotspot (or Captive Portal) Settings (continued)

Field	Description	
Pass-through IPs	The IP addresses that a user can go to without being redirected to the Redirect URL or without being authenticated, that is, the IP addresses that form the walled garden. You can enter up to three IP addresses with their subnet masks. The subnet masks must be entered in Classless Inter-Domain Routing (CIDR) notation.	
Authorized MAC Addresses	The MAC addresses for which authentication and redirection are bypassed. This option is particularly useful when wireless devices do not have browser capability, such as wireless VoIP phones. There are two methods to use the MAC Insertion Tool to add MAC addresses to the Authorized MAC Addresses table:	
	User defined MACs:	Manually enter one or more MAC addresses for which authentication and redirection must be bypassed. Then, click **<<< Add to list**.
	Connected clients:	Select one or more listed MAC addresses for which authentication and redirection must be bypassed. Then, click **<<< Add to list**.
	Note: To delete MAC addresses from the Authorized MAC Addresses table, select (highlight) one or more MAC addresses in the Authorized MAC Addresses table, then click **Delete highlighted**.	
Authentication Method	The method to perform user authentication. The pull-down menu lets you to make one of the following selections: • **No Authentication**. This is the default setting. • **Plain Key Authentication**. You must specify an authentication key. • **Shared Key Authentication**. You must specify an authentication key. • **RADIUS Authentication**. A RADIUS server is required (see "Configuring RADIUS Server Settings" on page 45).	
	Authentication Key	The authentication key for Plain Key Authentication and Shared Key Authentication.

6. Click **Save** or **Save to Flash & Activate** to save your settings.

   The Hotspot feature is now enabled and the first HTTP or HTTPS request will be redirected to the supplied Redirect URL. For information about wireless client separation, which is useful for hotspots and other public access situations, see "Configuring Wireless Client Separation" on page 58.

Configuring Advanced Wireless Settings

The advanced wireless settings normally do not need to be changed. The default advanced wireless settings usually work well.

To change the wireless access point's advanced wireless settings:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **Advanced** > **Wireless**. The Advanced (Wireless) Settings screen displays:

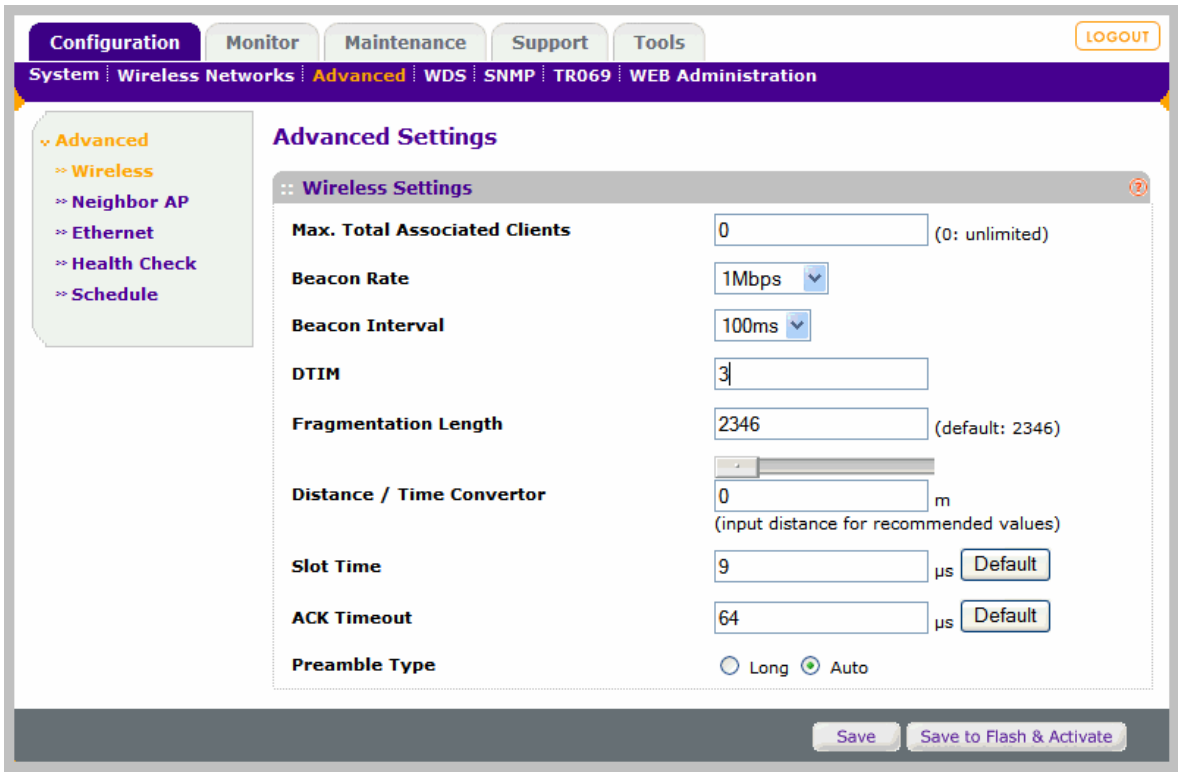


Figure 5-3

3. Specify the advanced wireless settings as explained in *Table 5-2*

4. Click **Save** or **Save to Flash & Activate** to save your settings.

Table 5-2. Advanced Wireless Settings

Field	Description
Max. Total Associated Clients	Specify the total maximum number of wireless clients that are allowed to connect to the wireless access point. The default setting is 0, which indicates a limitless number of wireless clients. **Note**: The "Configuring Advanced QoS Settings" on page 57 explains how to specify the maximum number of wireless clients that are allowed to connect to an individual SSID. The maximum total associated clients for the wireless access point overrides the sum of all wireless clients that are allowed to connect to all 16 SSIDs.
Beacon Rate	Select the beacon transmit bit rate from the pull-down menu: • **1Mbps**. This is the default setting. • **2Mbps**. • **5.5Mbps**. • **6Mbps**. • **11Mbps**.
Beacon Interval	Select the interval for each beacon transmission from the pull-down menu: • **100ms**.This is the default setting. • **250ms**. • **500ms**.
DTIM	The frequency for the beacon to include a Delivery Traffic Indication Message (DTIM) in milliseconds. The default setting is 3 milliseconds.
Fragmentation Length	This is the maximum packet size that is used for fragmentation. Packets larger than this size will be fragmented. The default is 2346.
Distance / Time Convertor	Use the on-screen slider to determine the recommended values for the slot time, ACK timeout, and CTS timeout (see below). You can also enter the distance in meters in the field below the slider, and then click in one of the three fields below to determine the recommended values. The default value is 0 meters.
Slot Time	The period in microseconds before packet transmission occurs from the wireless access point. (The slot time usually equals the maximum theoretical time for a packet to travel from the wireless access point to the target and back.) The default setting is 9 microseconds. Click **Default** to return the field to its default value.
ACK Timeout	The period in microseconds that is allowed for reception of an acknowledgement (ACK) packet by the wireless access point before the packet retransmission occurs. The default setting is 48 microseconds. Click **Default** to return the field to its default value.
Preamble Type	Select one of the following radio buttons: • **Auto**. A short transmit preamble provides better performance. Auto automatically handles both long and short preambles. The default setting is Auto. **Long**. A long transmit preamble may provide a more reliable connection or slightly longer range.

Configuring Neighbor AP Discovery

The Neighbor AP Discovery feature lets the wireless access point automatically register other wireless devices in its area and includes these devices in the Neighbor APs List (see “Viewing Neighbor APs Information” on page 76).

To configure the Neighbor AP Discovery feature:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **Advanced** > **Neighbor AP**. The Neighbor AP screen display (see *Figure 5-4* on page 101).

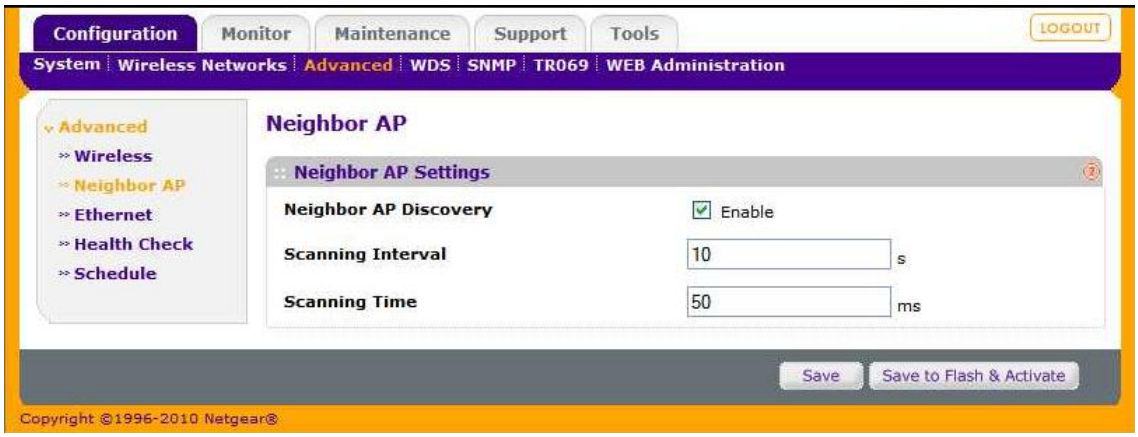


Figure 5-4

3. Specify the neighbor AP settings as explained in *Table 5-3*.

Table 5-3. Neighbor AP Settings

Field	Description
Neighbor AP Discovery	By default, the wireless access point automatically discovers other wireless devices in its area. Deselect the **Enable** checkbox to disable the Neighbor AP Discovery feature.
Scanning Interval	The frequency in seconds that the wireless access point scans the channels to discover neighboring APs. The default setting is 10 seconds.
Scanning Time	The time in milliseconds that the wireless access point scans a channel to discover neighboring APs. The default setting is 50 milliseconds.

4. Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring Wireless Bridging and Repeating

The wireless access point supports a wireless distributing system (WDS) that lets you build large bridged wireless networks. Examples of wireless bridged configurations are:

- **Point-to-point bridge**. The wireless access point communicates with another bridge-mode wireless access point. See “Configuring Point-to-Point Bridge Mode” on page 104.
- **Multi-point bridge**. The wireless access point is the “master” for a group of bridge-mode wireless access points. Then all traffic is sent to this “master,” rather than to the other wireless access points. See “Configuring Point to Multi-Point Bridge Mode” on page 106.
- **Repeater**. The wireless access point sends all traffic to the remote AP. See “Configuring Repeater Mode” on page 108.

To configure a wireless distributing system:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **WDS**. The WDS screen displays.

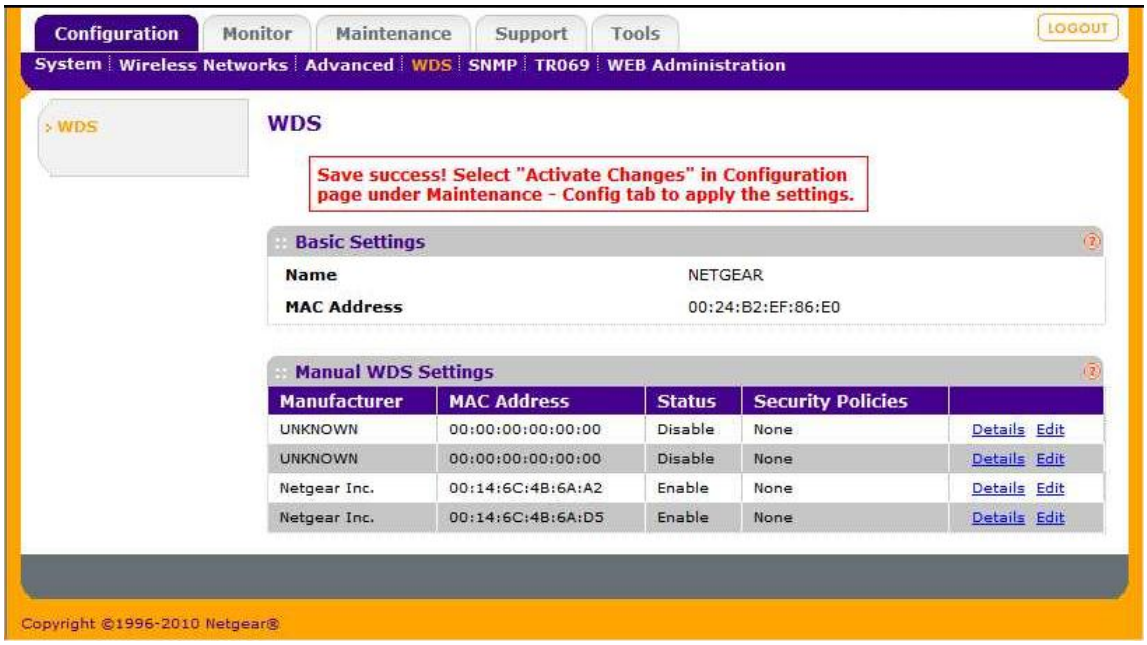


Figure 5-5

The Basic Settings section of the screen shows the AP name that you configured in “Configuring Basic System Settings” on page 19 and the wireless access point’s MAC address.

3. In the Basic Settings section of the screen, the Name and MAC Address of the access point are displayed. You configure the wireless distribution system. You can add up to four WDS

nodes. To configure WDS settings, click the **Edit** hyperlink to the right of one of the nodes in the WDS Settings table (see *Figure 5-5* on page 102). The Edit WDS screen displays.

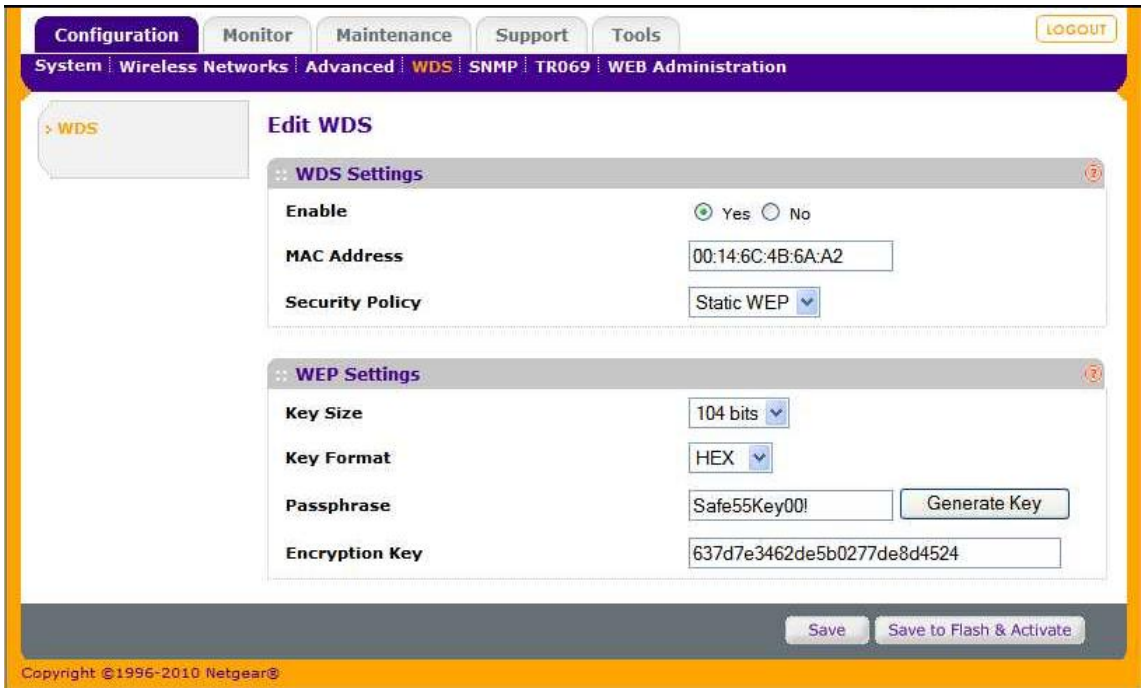


Figure 5-6

4. Specify the manual WDS settings as explained in *Table 5-4* and go to *step 5*.

Table 5-4. Manual WDS Settings

Field	Description
WDS Settings	
Enable	Select one of the following radio buttons: • **Yes**. The WDS node is enabled. • **No**. The WDS node is disabled.
MAC Address	The MAC address of the WDS node. **Note**: The manufacturer information in Manual WDS Settings table is based on the prefix of the WDS node's MAC address.

Table 5-4. Manual WDS Settings (continued)

Field	Description	
Security Policy	Select a security setting for the WDS node from the pull-down menu: • **None**. There is no security to protect communication over the WDS node. This is the default setting. • **Static WEP**. Pre-shared WEP key encryption without (RADIUS) authentication. When you select this option, the screen expands to let you configure the WEP settings.	
	WEP Settings	
	Key Size	This pull-down menu lets you select the encryption key size: • **40 bits (64-bit WEP)**. • **104 bits (128-bit WEP)**. • **128 bits (152-bit WEP)**.
	Key Format	This pull-down menu lets you select the encryption key format: • **ASCII**. The ASCII format applies only to encryption keys that are manually entered. • **HEX**. The HEX format applies both to keys that are manually entered and that are automatically generated. **Note**: For automatic encryption key generation, the strongest encryption is provided by a combination of a key with 128-bits and the HEX key format.
	Passphrase	Enter a passphrase. The passphrase length must be between 8 and 63 characters (inclusive). To generate an encryption key, click **Generate Key**.
	Encryption Key	Either manually enter a key or allow the key to be automatically generated by clicking **Generate Key**. • For ASCII format, depending on the key size selected, the manually entered encryption key must have a length of 5, 13, or 16 characters. • For HEX format, depending on the key size selected, the manually entered or automatically generated encryption key must have a length of 10, 26, or 32 characters. Wireless stations must use the key to access the wireless access point. **Note**: Not all wireless adapters support passphrase key generation.

5. Click **Save** or **Save to Flash & Activate** to save your settings.

Configuring Point-to-Point Bridge Mode

In point-to-point (P2P) bridge mode, the wireless access point communicates with another bridge-mode wireless station. Use wireless security to protect this communication. The

following figure shows an example in which two wireless access points (APs) function in point-to-point bridge mode.

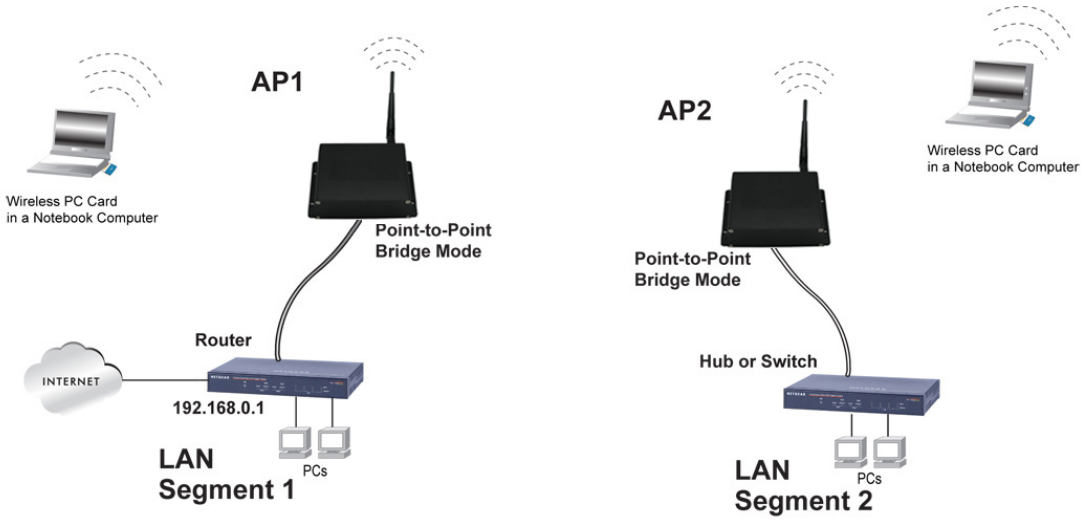


Figure 5-7

Note: *Figure 5-7* shows the WGAP150 with an external antenna, which does not come standard with the product.

To set up a point-to-point bridge configuration.

1. Configure the wireless access point (AP1 on LAN Segment 1 in *Figure 5-7*):
   a. Select **Configuration** > **WDS**.
   b. Next to WDS Mode, select the **Manual** radio button.
   c. Click the **Edit** hyperlink to the right of one of the nodes in the Manual WDS Settings table.
   d. On the Edit WDS screen, in the MAC Address field, enter the MAC address of the corresponding bridge-mode wireless access point (AP2 on LAN Segment 2 in *Figure 5-7*).
   e. Static WEP is supported. NETGEAR recommends that you configure static WEP to protect this communication. (You can do so on the Edit WDS screen.)
   f. Click **Save to Flash & Activate** to save and activate your settings.
2. Configure the other wireless access point (AP2 on LAN Segment 2 in *Figure 5-7* on page 105) in point-to-point bridge mode.

   AP1 must have AP2's MAC address in its Manual WDS Settings table and AP 2 must have AP1's MAC address in its Manual WDS Settings table.
3. Configure and verify the following for both wireless access points:
   - Verify the LAN network configuration of the wireless access points. Both must be configured to operate in the same LAN network address range as the LAN devices.

- Both wireless access points must use the same channel, authentication mode, and security settings.

4. Verify connectivity across LAN 1 and LAN 2.

   A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other computers or servers connected to LAN Segment 1 or LAN Segment 2.

Configuring Point to Multi-Point Bridge Mode

Set up a point to multi-point (P2MP) bridge only if the wireless access point (the WGAP150) is the “master” for a group of bridge-mode wireless access points. Then all traffic is sent to this “master,” rather than to the other wireless access points. Up to four profiles can be configured.

The following figure shows an example of a point to multi-point bridge mode configuration.

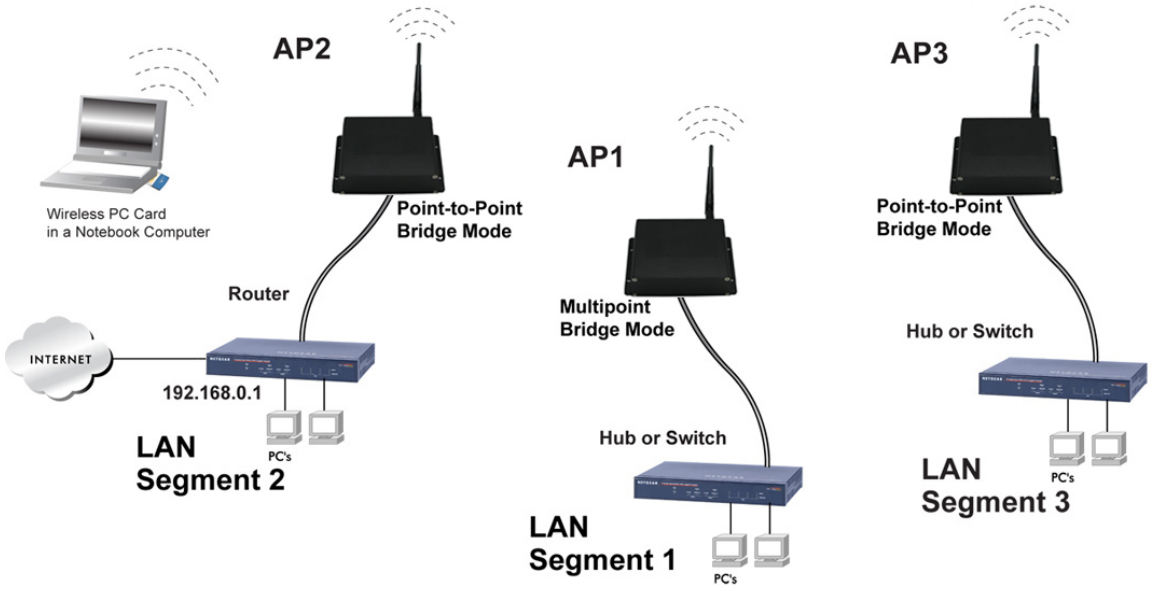


Figure 5-8

Note: *Figure 5-8* shows the WGAP150 with an external antenna, which does not come standard with the product.

To set up the point to multi-point bridge configuration:

1. Configure the wireless access point (AP1 on LAN Segment 1 in *Figure 5-8*):
   a. Select **Configuration** > **WDS**.
   b. Next to WDS Mode, select the **Manual** radio button.
   c. Click the **Edit** hyperlink to the right of one of the nodes in the Manual WDS Settings table.
   d. On the Edit WDS screen, in the MAC Address field, enter the MAC address of the corresponding wireless access points (AP2 on LAN Segment 2).
   e. Static WEP is supported. NETGEAR recommends that you configure static WEP to protect this communication. (You can do so on the Edit WDS screen.)
   f. Click **Save** to save your settings.
   g. Click the **Edit** hyperlink to the right of another node in the Manual WDS Settings table.
   h. On the Edit WDS screen, in the MAC Address field, enter the MAC address of AP3 on LAN Segment 3 in *Figure 5-8* on page 106).
   i. Static WEP is supported. NETGEAR recommends that you configure static WEP to protect this communication. (You can do so on the Edit WDS screen.)
   j. Click **Save to Flash & Activate** to save and activate your settings.
2. Configure AP2 on LAN Segment 2 (see *Figure 5-8* on page 106) in point-to-point bridge mode with the remote MAC address of AP1.
3. Configure AP3 on LAN Segment 3 (see *Figure 5-8* on page 106) in point-to-point bridge mode with the remote MAC address of AP1.
4. Verify the following for all wireless access points:
   - The LAN network configuration of the wireless access points are configured to operate in the same LAN network address range as the LAN devices.
   - Only AP1 on LAN Segment 1 is configured in point-to-multi-point bridge mode, and all others APs are configured in point-to-point bridge mode.
   - All point-to-point APs must have AP1's MAC address in their Manual WDS Settings table.
   - All APs must be on the same LAN. That is, the LAN IP addresses of all APs must be in the same network.
   - If using DHCP, all wireless access points should be set to obtain an IP address automatically (as a DHCP client). For more information, see "Configuring IP Settings" on page 20.
   - All wireless access points must use the same channel, authentication mode, and security settings.
5. Verify connectivity across the LANs:

- A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.

Note: You can extend this multi-point bridging configuration by adding additional wireless access points that are configured in point-to-point mode for each additional LAN segment. Furthermore, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.

Configuring Repeater Mode

Select this option to enable the wireless access point to operate as a repeater only without communication with other wireless clients. All traffic is sent to the remote or “downstream” wireless access point. Up to four profiles can be configured.

The following figure shows an example of a repeater mode configuration.

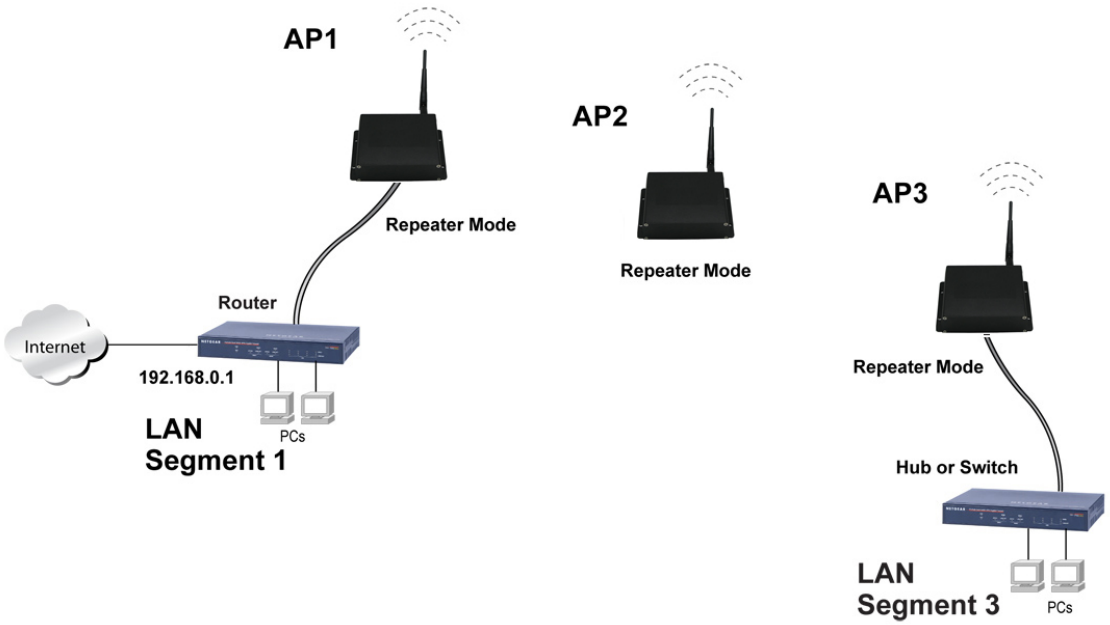


Figure 5-9

Note: *Figure 5-9* shows the WGAP150 with an external antenna, which does not come standard with the product.

To configure a LAN segment using the wireless access point in repeater mode:

1. Configure the wireless access point (AP1 on LAN Segment 1 in *Figure 5-9*):
   a. Select **Configuration** > **WDS**.
   b. Next to WDS Mode, select the **Manual** radio button.
   c. Click the **Edit** hyperlink to the right of one of the nodes in the Manual WDS Settings table.
   d. On the Edit WDS screen, in the MAC Address field, enter the MAC address of the corresponding wireless access points (AP2 on LAN Segment 2).
   e. Static WEP is supported. NETGEAR recommends that you configure static WEP to protect this communication. (You can do so on the Edit WDS screen.)
   f. Click **Save to Flash & Activate** to save and activate your settings.
2. Configure AP2 in LAN segment 2 with the MAC address of its “upstream” wireless access point (AP1).
3. In addition, configure AP2 with the MAC address of its “downstream” wireless access point (AP3 in LAN segment 3).
4. Configure AP3 with the MAC address of its “upstream” wireless access point (AP2).
5. Verify the following for all wireless access points:
   - The LAN network configuration of the wireless access points are configured to operate in the same LAN network address range as the LAN devices.
   - All APs must be on the same LAN. That is, the LAN IP addresses of all APs must be in the same network.
   - If using DHCP, all wireless access points should be set to obtain an IP address automatically (as a DHCP client). For more information, see “Configuring IP Settings” on page 20.
   - All wireless access points must use the same channel, authentication mode, and security settings.
6. Verify connectivity across the LAN.

Note: You can extend the repeating functionality by adding up to two more wireless access points that are configured in repeater mode. However, since repeaters communicate in half-duplex mode, the bandwidth decreases as you add repeaters to the network. Also, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.

6 Troubleshooting

This chapter provides information about troubleshooting your wireless access point. After each problem description, instructions are given to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the wireless access point on?

  Go to “Basic Functioning” on page 112.

- Have I connected the wireless access point correctly?

  Go to “Basic Functioning” on page 112.

- I cannot access the Internet or the LAN.

  Go to “You Cannot Access the Internet or the LAN from a Wireless-Capable Computer” on page 113.

- I cannot access the wireless access point from a browser.

  Go to “You Cannot Configure the Wireless Access Point from a Browser” on page 113.

- A time-out occurs.

  Go to “When You Enter a URL or IP Address a Time-out Error Occurs” on page 114.

- I cannot remember the wireless access point’s configuration password.

  Go to “Changing the Administrator Password and User Name” on page 66.

- I want to clear the configuration and start over again.

  Go to “Using the Reset Button to Restore Factory Default Settings” on page 116.

- The date or time is not correct.

  Go to “Problems with Date and Time” on page 116.

The wireless access point provides diagnostic tools that enable you to monitor the health of the system and to perform problem diagnoses. To use these diagnostic tools, go to “Using the Diagnostic Tools” on page 117.

Basic Functioning

After you turn on power to the wireless access point, the following sequence of events should occur:

- The power LED should be lit.
- The status LED should be lit.
- The LAN LED should be lit.
- The Wi-Fi LED should be lit.

If any of these conditions do not occur, see to the appropriate following section.

No LEDs are Lit on the Wireless Access Point

It takes a few seconds for the power LED to light up. Wait a minute and check the power LED status on the wireless access point. If the wireless access point has no power:

- Make sure that the Ethernet cable between the wireless access point and the PoE switch is properly connected at both ends.
- Make sure that the power cord of the PoE switch is plugged in to a working power outlet or power strip.
- Make sure you that your PoE switch is functioning normally.

The LAN LED is Not Lit

There is a hardware connection problem. Check these items:

- Make sure the cable connectors are securely plugged in at the wireless access point and the PoE switch.
- Make sure the connected device is turned on.
- Make sure that the correct cable is used. Use a standard Category 5 Ethernet patch cable.

The Wi-Fi LED Does Not Light Up During Wireless Activity

The wireless access point or the external antenna is not working.

- If the Wi-Fi light remains off while the wireless access point is transmitting or receiving data, disconnect the Ethernet cable from PoE switch and then plug it in again.
- Contact NETGEAR if the Wi-Fi light remains off while the wireless access point is transmitting or receiving data.

You Cannot Access the Internet or the LAN from a Wireless-Capable Computer

There is a configuration problem. Check the following:

- You may not have restarted the computer with the wireless adapter to allow TCP/IP changes take effect. Restart the computer.
- The computer with the wireless adapter may not have the correct TCP/IP settings to communicate with the network. Restart the computer and check that TCP/IP is set up properly for that network. The usual setting for Windows the Network Properties is set to "Obtain an IP address automatically."
- The wireless access point's default values may not work with your network. Check the wireless access point default configuration against the configuration of other devices in your network.
- Make sure that the SSID, network authentication, and data encryption settings of the computer with the wireless adapter are same as those of the wireless access point.
- Ping the IP address of the wireless access point to verify that there is a wireless connection between the computer with the wireless adapter and the wireless access point. If the ping fails, check the network configuration.
- Ping the default gateway to verify that there is a path from the computer with the wireless adapter to the default gateway. If the ping fails, check the network configuration or call the Internet service provider (ISP).

You Cannot Configure the Wireless Access Point from a Browser

Check the following:

- Make sure that the wireless access point is configured to accept configuration from a browser. Check the following:
  - Web management is enabled (see "Disabling Web Management Access Entirely" on page 81).
  - Web management access is properly configured, and if the Web Access Control feature is enabled, the IP address of your computer is in the Management IP table (see "Configuring Web Management Access" on page 78).
  - If you attempt to access the wireless access point form a wireless computer, the wireless access point is configured to accept Web management from a wireless client (see "Disabling Web Management Access from Wireless Clients" on page 80).
- The wireless access point is properly installed, LAN connections are OK, and it is powered on. Check that the LAN LED is on to verify that the Ethernet connection is OK.

- If you are using the NetBIOS name of the wireless access point to connect, ensure that your computer and the wireless access point are on the same network segment or that there is a WINS server on your network.
- If your computer uses a fixed (static) IP address, ensure that it is using an IP address in the range of the wireless access point. The wireless access point default IP address is 192.168.0.229 and the default subnet mask is 255.255.255.0.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when entering this information.

If the wireless access point does not save changes you have made in the Web configuration interface, check the following:

- When entering configuration settings, be sure to click the **Save** or **Save to Flash & Activate** button before moving to another screen or tab, or your changes are lost.
- Click the Refresh or Reload button in the Web browser. The changes might have occurred, but the Web browser might be caching the old configuration.

When You Enter a URL or IP Address a Time-out Error Occurs

A number of things could be causing this. Try the following troubleshooting steps.

- Check whether other computers on the LAN work properly. If they do, ensure that your computer's TCP/IP settings are correct. If you use a fixed (static) IP address, check the subnet mask, default gateway, DNS, and IP addresses of the wireless access point (see "Configuring IP Settings" on page 20).
- If the computer is configured correctly, but still not working, ensure that the wireless access point is connected and turned on. Connect to it and check its settings. If you cannot connect to the wireless access point, check the LAN and power connections, and check the Web management settings of the wireless access point (see "Disabling Web Management Access Entirely" on page 81, "Configuring Web Management Access" on page 78, and "Disabling Web Management Access from Wireless Clients" on page 80).
- If the wireless access point is configured correctly, check your Internet connection (for example, your cable modem) to make sure that it is working correctly.

Troubleshooting a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply.

Troubleshooting a TCP/IP network is made very easy by using the ping utility in your computer.

Testing the LAN Path to Your Wireless Access Point

You can ping the wireless access point from your computer to verify that the LAN path to your wireless access point is set up correctly.

To ping the wireless access point from a PC running Windows 95 or later:

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the field provided, type Ping followed by the IP address of the wireless access point, as in this example:

   `ping 192.168.0.229`
3. Click **OK**.

   You should see a message like this one:

   ```
   Pinging <IP address> with 32 bytes of data
   ```

   If the path is working, you see this message:

   ```
   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
   ```

   If the path is not working, you see this message:

   ```
   Request timed out
   ```

   If the path is not functioning correctly, you could have one of the following problems:

   - Wrong physical connections
     - Make sure the LAN LED is on. If the LED is off, follow the instructions in “The LAN LED is Not Lit” on page 112.
     - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and wireless access point.
   - Wrong network configuration
     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
     - Verify that the IP address for your wireless access point and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device.

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the Windows Run window, type:

PING -n 10 *IP address*

where *IP address* is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section display. If you do not receive replies:

- Check that your PC has the IP address of your router listed as the default wireless access point. If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC's Network Control Panel. Verify that the IP address of the router is listed as the default wireless access point as described in the online document that you can access from "Preparing Your Network" in Appendix B.
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your PC, enter that host name as the account name in the Basic Settings screen.

Using the Reset Button to Restore Factory Default Settings

To use the Reset button (see "Rear Panel" on page 11) to clear all data and restore the factory default values:

1. Push and hold the Reset button for about five seconds (you may have to push hard).
2. Release the Reset button. A few seconds later, only the power LED of the wireless access point remains on, indicating that the wireless access point has rebooted. After several minutes, the factory default configuration will be restored, and the wireless access point will be ready for use.

Note: After restoring the factory default configuration, the wireless access point's default LAN IP address will be **192.168.0.229**, the default login user name will be **admin**, and the default login password will be **password**.

Problems with Date and Time

The Basic screen that is accessible through the **Monitor** > **System** > **Basic** menus choices displays the current date and time of day. The wireless access point uses the Network Time Protocol (NTP) to obtain the current time from a Network Time Servers on the Internet that you specify in the Basic Settings screen (see "Configuring Basic System Settings" on

page 19). Each entry in the Event Log is stamped with the date and time of day. Problems with the date and time function can include:

- Date and time shown is Fri Dec 31 00:00:00 1999 or a similar incorrect date and time. Cause: The wireless access point has not yet successfully reached the Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the wireless access point, wait at least five minutes and check the date and time again.
- The day is correct or one day ahead or behind, and the hours are ahead or behind. Cause: You have selected an incorrect time zone for your area. Specify the correct time zone in the Basic Settings screen (see “Configuring Basic System Settings” on page 19).

Using the Diagnostic Tools

You can perform diagnostic tasks such as pinging an IP address, tracing a route to an IP address, and performing a DNS lookup.

Health Check

The health check consist of a ping packet request that is sent continuously to a host that you specify at an interval that you specify.

To configure a health check:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.
2. Select **Configuration** > **Advanced** > **Health Check**. The Health Check screen displays (see *Figure 6-1* on page 117).

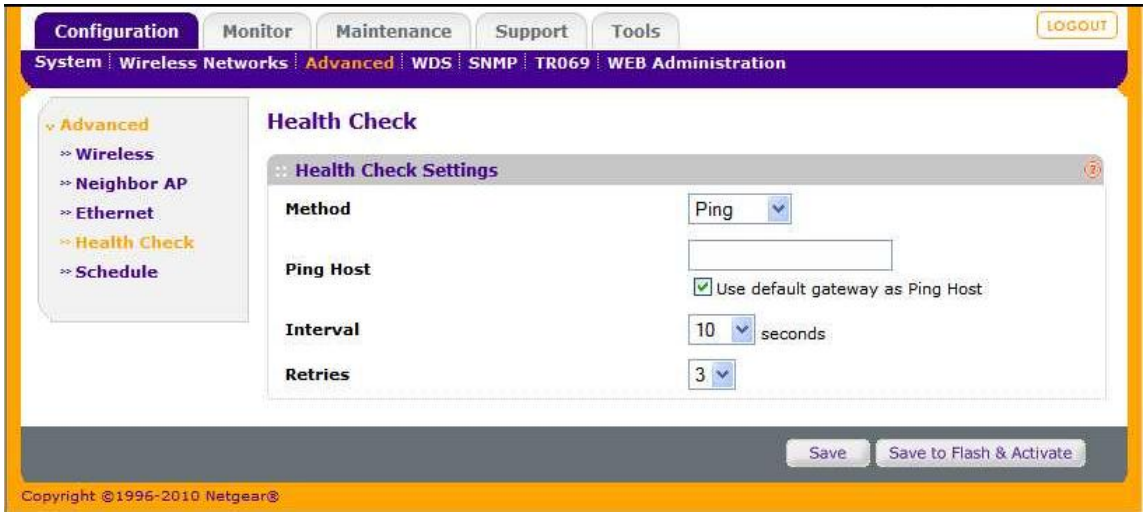


Figure 6-1

3. From the **Method** pull-down menu, select **Ping**. The screen expands, enabling you to configure ping fields.
4. Specify the fields that are explained in the following table.

Table 6-1. Health Check Settings

Field	Description
Ping Host	The IP address of the host to which the continuous ping should be sent. By default, the IP address of the default gateway that you selected in "Configuring IP Settings" on page 20 is used as the ping host, and the Ping Host field is masked out. Deselect the **Use default gateway as Ping Host** checkbox to specify a host in the Ping Host field.
Interval	The interval in seconds at which the host is pinged. You can select 10 (default), 30, 60, or 120 seconds.
Retries	The number of times that the wireless access point attempts to ping the host after the initial attempt fails. You can select 1, 3 (default), 5, or 7. If all pings fail, the connection between the wireless access point and the host is terminated, and the Event Log will show the message "Health Check: Link Down." If the connection comes up again, the Event Log will show the message "Health Check: Link Up."

5. Click **Save** or **Save to Flash & Activate** to save your settings.

Using the Ping, Traceroute, and NsLookup Utility

These diagnostic tools are not required if the wireless access point functions normally. As port of a troubleshooting procedure, you can send a ping packet, traceroute, or Nslookup request to an IP address or host name.

To use diagnostic tools:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using whatever LAN address, user name, and password you have chosen for the wireless access point.

2. Select **Tools**. The Diagnostic Tools screen displays.

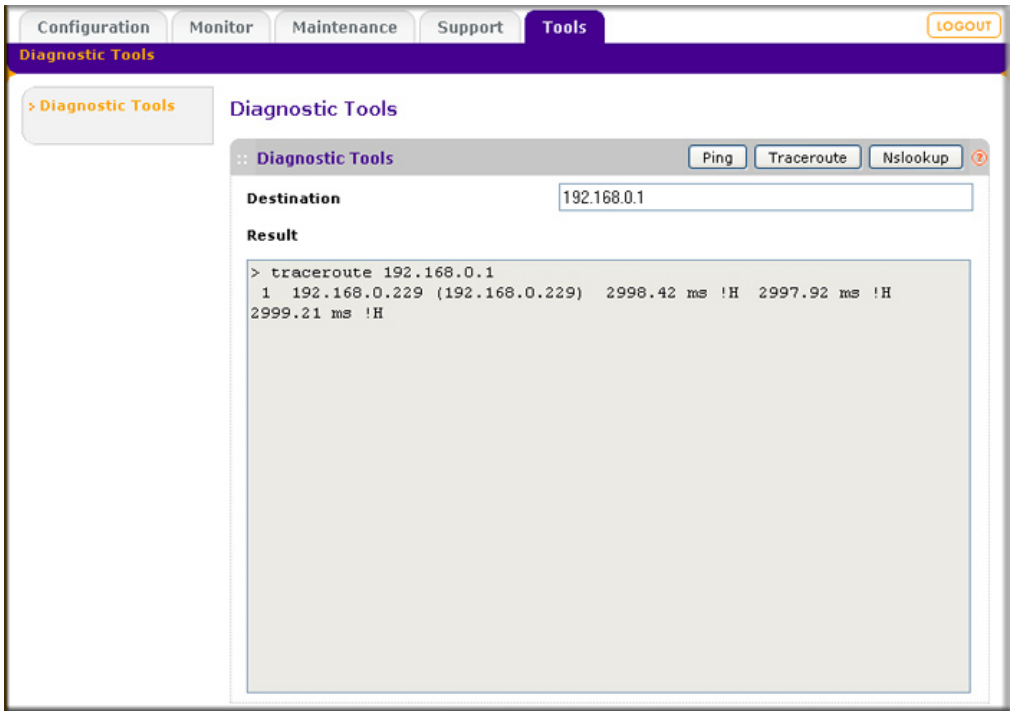


Figure 6-2

3. Enter an IP address or domain name in the Destination field.W
4. From the Diagnostic Tolls menu, select one of the following options:
   - **Ping**. Ping a device. If the request times out (no reply is received), it usually means that the destination is unreachable. However, some network devices can be configured not to respond to a ping.
   - **Traceroute**. Trace a route. Lists all routers between the source (this wireless access point) and the destination IP address.
   - **Nslookup**. Query a DNS server. A Domain Name Server (DNS) converts the Internet name (for example, www.netgear.com) to an IP address. If you need the IP address of a Web, FTP, Mail or other server on the Internet, you can request a DNS lookup to find the IP address.

   The results are displayed in the Results window.

Downloading Debug Information

Debug information will assist NETGEAR technical support to find a solution when you are experiencing technical issues with the wireless access point.

To download the debug file:

1. Log in to the wireless access point at its default LAN address of **http://192.168.0.229** with its default user name of **admin** and default password of **password**, or using

whatever LAN address, user name, and password you have chosen for the wireless access point.

2. Select **Maintenance** > **Misc**. The Miscellaneous screen displays.

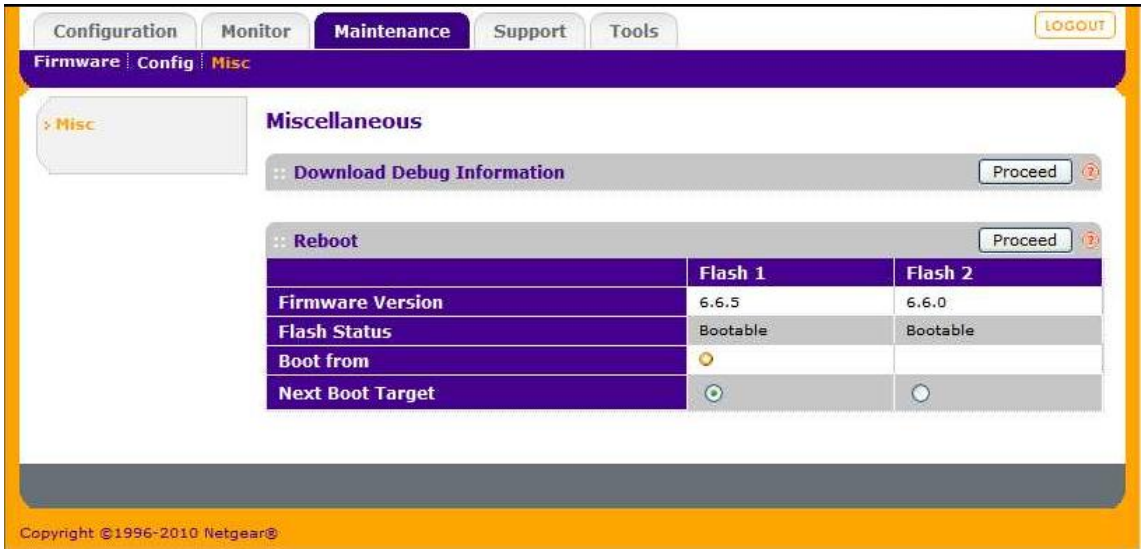


Figure 6-3

3. Next to Download Debug Information, click the **Proceed** button.
4. Save the debug.dump file to a location on your computer and follow the instructions of NETGEAR technical support.

Technical Specifications

A

This appendix provides technical specifications and factory default settings for the WG102-500, WGAP150 ProSafe™ 802.11g Wireless Access Point.

General Specifications

Specification	Description
Network Management	• Web-based configuration and status monitoring • Telnet support • SNMP support
Status LEDs	• Power • Status • Ethernet • Wireless (Wi-Fi)
Power Source	12V 1.5A power adapter
	Optional: Power Over Ethernet (PoE) conform 802.3af.
Power Consumption	~12 W
Transmission Power	27 dBm **Note**: The maximum transmission power varies and is based on your selection of the country or region on the 802.11b/g/n Profile screen (see "Configuring 802.11b/g Wireless Settings" on page 25) to ensure local regulatory compliance.
Physical Specifications	Dimensions (length x width x height): 220mm x 132mm x 40mm 8.66" x 5.20" x 1.58"
	Weight: 420 gr. 0.93 lb..
Environmental Specifications Operating temperature: Operating humidity:	 0°C to 50°C (32°F to 131°F) 15-90%, non-condensing

Specification	Description
Maximum Computers Per Wireless Network	Limited by the amount of wireless network traffic generated by each node. Typically 20-30 nodes.
Radio Data Rates 802.11b and g	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
802.11b,g Operating Frequencies and Channels	2.412 ~ 2.462 GHz (North America), Channels 1-11 2.412 ~ 2.472 GHz (Europe including France and Spain, and Japan), Channels 1-13
802.11 Security	40-bits (64-bit WEP), 104 bits (28-bit WEP), and 128-bits (152-bit WEP) data encryption; WPA and WPA2

Default Factory Settings

When you first receive your wireless access point, the default factory settings are set as shown below. You can restore these defaults with the Reset button on the rear panel (see “Rear Panel” on page 11).

Table 0-1.

Feature	Factory Default Settings
User Name (case sensitive)	admin
Password (case sensitive)	password
Operating Mode	Bridge
Access Point Name	NETGEAR
Built-in DHCP Server	DHCP server enabled, using the default IP address
IP Configuration	IP Address: 192.168.0.229 Subnet Mask: 255.255.255.0 Gateway: 0.0.0.0
Network Name (SSID)	16 SSIDs: NETGEAR - 0, NETGEAR - 1, NETGEAR - 2, and so on to NETGEAR - 15
Broadcast Network Name (SSID)	Enabled
WEP/WPA	Disabled
MAC Access Control	Disabled
Restricting connectivity based on MAC Access Control List	Disabled
Time Zone	Coordinated Universal Time (UTC)

Table 0-1.

Feature	Factory Default Settings
SNMP	Enabled
VLAN (802.1Q)	Disabled
WMM Support	Enabled
Mesh Connector Bridging	Disabled

Related Documents

B

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Using Microsoft Vista and Windows XP to Manage Wireless Network Connections	*http://documentation.netgear.com/reference/enu/winzerocfg/vistaxpconfig.pdf*
ITCP/IP Networking Basics	*http://documentation.netgear.com/reference/enu/tcpip/index.htm*
Wireless Networking Basics	*http://documentation.netgear.com/reference/enu/wireless/index.htm*
Preparing Your Network	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Virtual Private Networking Basics	*http://documentation.netgear.com/reference/enu/vpn/index.htm*
Glossary	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

Index

Numerics

64-bit, 128-bit, and 152-bit encryption keys 8
802.11b 26
802.11e 9, 57
802.11g 8, 9, 10, 26

A

access control, trusted wireless stations 9, 51
access point
  domain name 20
  location name 20
  name 20, 122
  operating modes 20
  rear-panel ports and LEDs 11
access, restricting by MAC address 50
account name 116
accounting, RADIUS servers 45, 47
ACK (acknowledgement) timeout 100
activation of changes, scheduling 64
ActiveX 114
activity log 68
administrative status, SSID 27
administrator
  password 66
  user name 67
Advanced Encryption Standard (AES) 35
antenna, external
  connector 11
  orientation 14
area of coverage 7
ARP (Address Resolution Protocol) 56
attached devices, monitoring with SNMP 85
authentication
  methods for HTTP and HTTPS redirection 98
  network 35
  RADIUS
    alternate servers 48
    EAPOL versions 48
    servers 45, 46
  SNMP agent 90
  SNMPv3 user 90
  See also WEP
  See also WPA (WPA and WPA2)
auto channel selection, scheduling 92
auto-detecting, Ethernet link speed 96
automatic configuration, using DHCP 8, 20, 24, 52

B

backing up, configuration file 62
bandwidth
  allocation 9
  decreasing in WDS 109
  setting limits 54
basic settings, configuring 18
basic wireless information 75
beacon rate and interval 100
bridge mode 20
bridge priority (STP) 20
bridging and repeating, *See* wireless distribution system (WDS)
broadcasting, wireless network name (SSID) 29
browser, recommended 17
BSS (Basic Service Set) 8, 36
BSSID (Basic Service Set Identifier)
  configuring for security profile 28
  description 8
  number supported 35

C

cables, Ethernet (cat.5 UTP straight-through) 10
captive portals, *See* hotspots
CBC-DES, SNMP agents 90
changing administrative settings
  password 66
  user name 67
channels, wireless
  fixed 26
  See also RF channels
  spacing 14
clients
  broadcast/multicast packet separation (wireless) 59
  current number (wireless) 75
  details (wireless) 76

DHCP 8, 20
general separation (wireless) 36, 58
MAC address (wireless) 76
manufacturer (wireless) 76
maximum number per SSID 57
separation between SSIDs 59
unicast packet separation (wireless) 59
communities, SNMP 86
configuration file
backing up 62
erasing 63
restoring 62
saving 63
configuring basic settings 18
convertor (on-screen), distance/time 100
country and region, operation 26
coverage, wireless network 7

D

data encryption
See WEP
See WPA (WPA and WPA2)
data rates, transmission 30, 122
date, troubleshooting 116
debug information, downloading 119
default
configuration 63
factory settings 122
gateway 21
IP address 17, 22
IP addresses 122
login name 114
password 17, 122
subnet mask 17, 21, 122
user name 17, 122
VLAN, for security profile 27, 29
destination port, wireless traffic filtering 56
DHCP (Dynamic Host Configuration Protocol)
clients 8, 20
server 24
server, alternate 52
diagnostic tools 117
disabling
access from wireless clients 80
radio 26
DNS (Domain Name System) servers 21, 24, 53
documentation, online 93
documents, reference 125
Domain Name System, *See* DNS
domain name, wireless access point 20
downstream bandwidth limits 54
DTIM (Delivery Traffic Indication Message), beacon 100
dynamic IP address 8

E

EAPOL (Extensible Authentication Protocol over LAN), versions 48
encryption of data
key format (WEP) 40
key generation (WEP) 40, 104
See also WEP
See also WPA (WPA and WPA2)
erasing, configuration file 63
ESS (Extended Service Set) 36
Ethernet
cable 10
cabling requirements 14
interface 9
link configuration 95
link speed 96
Ethernet path cost (STP) 20

F

factory settings 122
features, list of 8
filtering, protocols 56
firmware
flash memory 65
upgrading 65
version 71, 74
flash management information 74
flash memory, firmware storage 8
form, recording wireless network settings 36
fragmentation
length 100
packets 100
frequencies
operating 122
See also RF channels
full-duplex mode 96

G

gateway
default 21
IP address for DHCP clients, alternate 53
IP address for DHCP clients, default 24
pinging 118
general specifications 121
graphical user interface (GUI) 18

H

half-duplex mode 96, 109
hardware, rear panel ports and LEDs 11
hidden mode 9
HMAC-MD5 and HMAC-SHA, SNMPv3 users 90
hotspots 8
  redirecting HTTP and HTTPS requests 97
  settings 96
HTTP (Hypertext Transfer Protocol, using for web access 79
HTTP and HTTPS redirecting 97
HTTPS (Hypertext Transfer Protocol over Secure Socket Layer), using for web access 79

I

ICMP (Internet Control Message Protocol) 56
infrastructure mode 26
installation order 15
interference
  channels 14
  sources of 14
Internet browsing, troubleshooting 113
IP addresses
  default 17, 22, 122
  DHCP ranges 24
  DNS severs
    alternate 53
    default 24
  dynamic 8
  gateway, alternate 53
  gateway, default 24
  L2TP server 83
  L2TP tunnel address 83
  LAN 23
  pass-through, hotspots 98
  RADIUS servers 46
  receiving SNMP traps 86
  See also subnet masks
  SNMP manager 88
  source and destination for filtering 56
  static 21
  syslog server 70
  viewing 72
  web management control 80
IP settings
  basic 20
  configuring 20
  DHCP clients 8, 20
  DHCP server 24
  DHCP server, alternate 52
  viewing current settings 72

J

Java and Javascript 114

K

key size, WEP 41, 104

L

L2TP
  server address 83
  tunnel address 83
  tunnel information 73
  tunnel management, configuring 82
LAN
  configuration requirements 14
  IP address and subnet mask 23
  LED 16, 112
  path, troubleshooting 115
  port 11
  settings, configuring 23
LEDs
  front panel, description of 12
  LAN 16, 112
  Power 16, 112
  Status 16
  troubleshooting 112
  Wi-Fi 16, 112
limiting bandwidth 54
location
  name 20
  wireless equipment 13
log, activity 68
logging in 17
login name, default 114
losing, wireless connection 52

M

MAC addresses 51
  bypassing for hotspots 98
  restricting access 34, 50
  source and destination for filtering 56
  trusted and refused 50
  WDS node 103
  wireless client 76
management tasks 91, 92
management VLANs 20
management, remotely
  disabling web access from wireless clients 80
  disabling web management entirely 81
  L2TP tunnel 82
  overview of methods 78
  port for web access 79
  SNMP 85

Telnet 84
web access, configuring 78
maximum number, wireless clients 7, 100
maximum retransmission, RADIUS servers 47
maximum transmission power 121
mesh connector bridging 57
methods for remote management 78
MIB objects 88, 90
mixed mode (WPA+WPA2 and WPA-PSK+WPA2-PSK), *See* WPA (WPA and WPA2)
modes, operating, wireless access point 20
multicast, filter and rate 30
multiple access points
using different channels 26
using the same SSID 76

N

name
default network (SSID) 122
network (SSID) 29
wireless access point 20, 122
wireless access point location 20
neighbor AP discovery
neighbor AP list 77
settings 101
status 77
network
authentication 35
basic wireless settings 27
nslookup 119
NTP (Network Time Protocol) server 20
number
associated clients per SSID 57
wireless clients, maximum 7, 100
WLANs in use 75

O

online documentation, accessing 93
on-screen convertor, wireless distance/time 100
open system (WEP) 41
operating frequencies, *See* RF channels
operating modes, wireless access point 20
order of installation and configuration 15
output power, transmission (TX) 26

P

packets, fragmentation 100
passphrases
See WEP
See WPA (WPA and WPA2)
pass-through IP addresses, hotspots 98
password
changing 66
default 17, 122
L2TP/PPP 83
restoring 63, 116
SNMP agent authentication 90
SNMPv3 user authentication 90
physical specifications 121
pinging
any destination address 118, 119
default gateway 118
hosts 118
wireless access point 113, 114
placement, wireless equipment 13
point to multi-point bridge mode 8, 102, 106
point-to-point bridge mode 8, 102, 104
policy, radio mode (802.11b, 802.11g) 26
port (LAN port) 11
port numbers
Radius servers 46
syslog server 70
portals, captive, *See* hotspots
ports, external antenna, LAN, and power 11
power
adapter 121
connector 11
consumption and maximum transmission 121
LED 16, 112
Power over Ethernet, *See* PoE
PPPoE (PPP over Ethernet), settings 21
pre-shared key (PSK), *See* WPA (WPA and WPA2)
primary DNS server
alternate 53
default 24
priority, bridge (STP) 20
private SNMP community 88
protocols, filtering 56
protocols, SNMPv3 authentication
CBC-DES (SNMP agents) 90
HMAC-MD5, HMAC-SHA (SNMPv3 users) 90
public SNMP community 88

Q

QoS (Quality of Service)
advanced settings 57
features, list of 9
levels (gold, silver, bronze) 29
upstream and downstream bandwidth limits 54
wireless traffic filtering 55
WMM 57

R

radio
- disabling 26
- policy mode (802.11b, 802.11g) 26

RADIUS settings, configuring
- alternate servers (primary and secondary) 48
- default servers (primary and secondary) 45
- reauthentication time 47
- shared key (or secret) 47

range
- quidelines for wireless equipment 13
- wireless 7

real-time status, wireless access point 72

rear panel ports, description 11

reauthentication time, RADIUS servers 47

rebooting
- restoring default configuration 63
- scheduling 92
- without restoring default configuration 64

redirecting
- hotspots, HTTP and HTTPS requests 97
- web access, HTTP to HTTPS 79

reference documents 125

region and country of operation 26

registration card 10

rekeying
- *See* WEP
- *See* WPA (WPA and WPA2)

remote management
- disabling access from wireless clients 80
- disabling web management entirely 81
- L2TP tunnels 82
- overview of methods 78
- SNMP 85
- Telnet 84
- web access protocols 79
- web management access 78

repeater mode, wireless 8, 102, 108

request interval, RADIUS servers 47

requirements, before installing 10

Reset button 11, 63, 116, 122

restoring
- configuration file 62
- default configuration 63
- password 63, 116

RF channels
- current channel in use 75
- operating frequencies 122
- selection 26

roaming 36, 76

router mode 20

S

Save button 18

Save to Flash & Activate button 18

saving, configuration file 63

scanning time and interval, neighbor AP discovery 101

scheduling
- activation of changes 64
- auto channel selection 92
- rebooting 92

secondary DNS server
- alternate 53
- default 24

secret (or shared key), RADIUS servers 47

security policy, configuring for security profile 28

security profiles
- creating and configuring 37
- description 9, 35
- enabling 29
- settings, basic 27

security, wireless
- broadcasting SSID 34
- multiple BSSIDs combined with VLANs 34
- options 33
- restricting access by MAC address 34, 50
- *See* WEP
- *See* WPA (WPA and WPA2)

sending activity log 69

separation
- between SSIDs 59
- broadcast/multicast packets 59
- general for wireless clients 36, 58
- unicast packets 59

server
- alternate DHCP 52
- default DHCP 24
- SNMP 86

Service Set Identifiers, *See* SSIDs

settings
- advanced QoS 57
- advanced wireless LAN 98
- basic IP 20
- basic security profile 27
- basic wireless 24
- basic wireless network 27
- DHCP server
  - alternate 52
  - default 24
- Ethernet link 95
- hotspots 96
- L2TP tunnels 82
- LAN 23
- neighbor AP discovery 101
- PPPoE 21

QoS levels 29
RADIUS servers
alternate (primary and secondary) 48
default (primary and secondary) 45
security profiles 37
SNMP 85
static IP 21
WDS 102
WEP 40, 41
WPA and WPA-PSK 41
WPA+WPA2 and WPA-PSK+WPA2-PSK mixed modes 44
WPA2 and WPA2-PSK 43
shared key
RADIUS servers 47
WEP 41
slot time 100
SNMP (Simple Network Management protocol)
communities, configuring 86
remote management, configuring 85
support 8
users, configuring 88
source port, wireless traffic filtering 56
specifications, general 121
speed, Ethernet link 96
SSIDs
administrative status 27
broadcasting name 29
configuring for security profiles 27
default name 29, 122
description 8
matching 26, 29
renaming 29
separation between 59
standards
802.11e 9, 57
802.11g 8, 9, 10
static IP address 21
Status LED 16
STP (Spanning Tree Protocol), enabling 20
subnet masks
configuring 21
default 17, 122
DHCP clients 24
L2TP tunnel 83
LAN 23
SNMP manager 88
viewing 72
web management control 80
support registration card 10
syslog server 69
system
information 70
requirements 10
time and time zone 72

T

tasks, management 91, 92
TCP (Transmission Control Protocol) 56
TCP/IP network, troubleshooting 114
technical support 2
downloading debug information 119
Telnet, configuring 84
tertiary DNS server
alternate 53
default 24
time and time zone
selecting 20
troubleshooting 116
viewing 72
time-out error 114
TKIP (Temporal Key Integrity Protocol) 35
traceroute 119
trademarks 2
traffic filtering, wireless
configuring 55
protocols 56
source and destination IP addresses 56
source and destination ports 56
transmission (TX) output power 26, 121
transmission data rate 30
traps, SNMP 86
troubleshooting
basic functioning 112
cannot access the Internet or LAN 113
cannot configure from a browser 113
date 116
debug information 119
diagnostic tools 117
LAN LED 112
LAN path 115
nslookup 118
pinging 113, 114, 118
Power LED 112
restoring factory default settings 116
TCP/IP settings 113
time and time zone 116
time-out error 114
traceroute 118
Wi-Fi LED 112
trusted 51
trusted MAC addresses of wireless clients 51

U

UDP (User Datagram Protocol) 56

up time 72
upgrading, firmware 65
upstream bandwidth limits 54
user name
  changing 67
  default 17, 122
  L2TP/PPP 83
  SNMPv3 user 90
users
  number of wireless 7
  SNMPv3, configuring 88

V

version, firmware 71, 74
VID (VLAN ID), wireless client 76
viewing
  activity log 68
  basic wireless information 75
  flash management information 74
  L2TP tunnel information 73
  system information 70
  WDS neighbor AP information 76
  wireless clients information 75
VLANs
  configuring default for security profile 27, 29
  IDs 36
  management 20
  support 9
  web management over L2TP tunnel 83

W

web browsers, recommended 17
web interface menu 18
web management 78
  access protocols 79
  allowing control 80
  configuring access 78
  disabling access entirely 81
  disabling access from wireless clients 80
  VLAN ID for L2TP tunnel 83
WEP
  dynamic WEP
    configuring 41
    key size 41
    rekeying period 41
  static WEP
    configuring 40
    key generation 40
    key size and format 40
    open system 41
    passphrase 40
    shared key 41
    supported keys 8
  static WEP for WDS
    configuring 104
    key generation 104
    key size and format 104
    passphrase 104
    supported keys 8
  types of encryption 35
Wi-Fi LED 16, 112
Wi-Fi Multimedia, *See* WMM
Wi-Fi protected access version 2 *See* WPA2
Wi-Fi protected access, *See* WPA
wired equivalent privacy, *See* WEP
wireless bridging and repeating, *See* wireless distribution system (WDS)
wireless clients
  broadcast/multicast packet separation 59
  detailed information 76
  general separation 36, 58
  MAC address 76
  manufacturer 76
  maximum number of 100
  number of 7
  separation between SSIDs 59
  trusted 51
  unicast packet separation 59
  VID 76
  viewing information 75
wireless connection
  losing 52
wireless distribution system (WDS)
  description 8
  neighbor AP information 76
  point to multi-point bridge mode 8, 102, 106
  point-to-point bridge mode 8, 102, 104
  settings 102
  wireless repeater mode 8, 102, 108
  wireless security 104
wireless network
  adapters, 802.11b and 802.11g 15
  area of coverage 7
  broadcasting name (SSID) 29
  default name (SSID) 29, 122
  equipment, placement and range 13
  form to record settings 36
  range 7
  renaming SSID 29
wireless security
  broadcasting SSID 34
  multiple BSSIDs combined with VLANs 34
  options for security 33
  restricting access by MAC address 34, 50
  See WEP
  See WPA (WPA and WPA2)

WDS, static WEP 104
wireless settings
advanced wireless 98
basic 24
basic wireless network 27
wireless traffic filtering
configuring 55
source and destination ports 56
WMM (Wi-Fi Multimedia)
802.11e 9, 57
configuration 57
description 9
WPA (WPA and WPA2)
types of encryption 8, 35
WPA and WPA-PSK
configuring 41
passphrases 42
pre-shared key 42
RADIUS servers 42
rekeying period 42
user authentication 42
WPA2 and WPA2-PSK
configuring 43
passphrases 43
pre-shared key 43
RADIUS servers 43
rekeying period 43
user authentication 43
WPA+WPA2 and WPA-PSK+WPA2-PSK
mix.modes
configuring 44
passphrases 44
pre-shared key 44
RADIUS servers 44
rekeying period 44
user authentication 44